SIEMENS

SIMATIC

Prozessleitsystem PCS 7 Kompendium Teil F - Industrial Security (V8.0)

Projektierungshandbuch

Gültig für PCS 7 V8.0 (aktualisiert für V8.0 SP1)

11/2013

A5E32334448-AB

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E32334448-AB
Ⓟ 11/2013 Änderungen vorbehalten

Inhaltsverzeichnis

1 Vorwort

Gegenstand des Handbuchs

SIMATIC PCS 7, als ausgeprägt offenes System, gewährleistet ein hohes Maß der Adaption an verschiedenste Kundenbedürfnisse. Die Systemsoftware bietet dem Projekteur hierfür viele Freiheiten in Bezug auf den Projektaufbau sowie die Gestaltung des Programms und der Visualisierung.

Die Erfahrung hat gezeigt, dass sich spätere Modernisierungen oder Anlagenerweiterungen wesentlich einfacher gestalten, wenn von vorn herein weitestgehend "PCS 7 konform" projektiert wird. Das heißt, gewisse Grundregeln sollen zwingend eingehalten werden, um auch zukünftig die gegebenen Systemfunktionen optimal nutzen zu können.

Dieses Handbuch dient als Kompendium zusätzlich zur Produktdokumentation rund um SIMATIC PCS 7. Grundlegende Arbeitsschritte der Projekterstellung und Parametrierung werden in Form von Handlungsanweisungen mit zahlreichen Abbildungen beschrieben.

Das Kompendium spiegelt geradlinig den empfohlenen Weg durch die Projektierung wieder, wobei zahlreiche Praxiserfahrungen ausgewertet werden. Die Beschreibung geht nicht bis in die Applikation selbst, sondern bezieht sich auf den Umgang mit dem Projekt und die Parametereinstellungen der enthaltenen Komponenten.

Das Kompendium ist in die folgenden Teile gegliedert:

- Projektierungsleitfaden inkl. Checkliste
- Process Safety inkl. zwei Checklisten
- Technische Funktionen mit SFC-Typen
- Betriebsführung und Wartung inkl. Checkliste
- Hardware-Aufbau inkl. Checkliste
- Industrial Security

Gültigkeit

Dieses Handbuch berücksichtigt die in der SIMATIC PCS 7-Dokumentation und im Speziellen die im "Sicherheitskonzept PCS 7 & WinCC" enthaltenen Aussagen. Es kann bei mit SIMATIC PCS 7 automatisierten Anlagen und Projekten genutzt werden.
Der Projektierungsleitfaden ist gültig ab SIMATIC PCS 7 V8.0 (aktualisiert für V8.0 SP1).

SIMATIC PCS 7 Manual Collection

Die Gesamtdokumentation von PCS 7 steht Ihnen kostenlos und mehrsprachig im MyDocumenationManager als Manual Collection über die Internet-Seite http://support.automation.siemens.com/WW/view/de/59538371 oder im PDF-Format über www.siemens.de/pcs7-dokumentation zur Verfügung.

Gegenstand von Teil F "Industrial Security"

Im Produktions- und Automatisierungsumfeld geht es in erster Linie um die Verfügbarkeit der Anlage. Der Schutz von Informationen oder Daten stehen erst an zweiter Stelle. Die Industrial Security darf im Automatisierungsumfeld nicht auf Informationssicherheit reduziert werden. Die übermittelten Informationen steuern und überwachen unmittelbar und deterministisch physikalische und/oder chemische Prozesse. Aus diesem Grund ist bei einer Betrachtung der möglichen IT-bedingten Schäden im Produktionsumfeld die eigentliche Information vergleichsweise unwichtig (Ausnahme: Betriebsgeheimnisse wie z. B. Rezepturen). Wichtig ist die durch den Einsatz von Automatisierungstechnik mögliche (und gewollte) unmittelbare Auswirkung von Informationen auf die Prozessführung und Prozessüberwachung. Wird dieser Informationsfluss gestört, ist eine ganze Reihe von Konsequenzen zu erwarten:

- Eingeschränkte Prozessverfügbarkeit bis hin zum Verlust der Prozesskontrolle
- Unmittelbare Fehlsteuerungen
- Anlagenstillstände, Produktionsausfälle und Produktverunreinigungen
- Schäden an der Anlage
- Gefahren für Leib und Leben
- Gefahren für die Umwelt
- Verstöße gegen gesetzliche oder behördliche Auflagen
- Strafrechtliche oder zivilrechtliche Konsequenzen
- Verlust an öffentlichem Ansehen (Imageschaden)
- Vermögensschäden

Daraus folgt, dass sich die Schutzziele in der Prozessautomatisierung und in der traditionellen Informationstechnologie wesentlich unterscheiden. Bei Büroanwendungen steht Vertraulichkeit und Datenschutz im Vordergrund. Bei Automatisierungssystemen stehen die unbedingte Aufrechterhaltung der Betriebssicherheit und der Schutz von Leib und Leben an erster Stelle. Die entscheidende Voraussetzung hierfür ist die Wahrung der Verfügbarkeit der Anlage und damit die uneingeschränkte Kontrolle über den Prozess. Die Konsequenz hieraus ist, dass die im Büroumfeld bewährten Methoden und Ansätze nicht eins zu eins in der Automatisierungstechnik einsetzbar sind.

Dieses Handbuch dient als Kompendium zusätzlich zur Produktdokumentation zu SIMATIC PCS 7. Grundlegende Arbeitsschritte der Projekterstellung und Parametrierung werden in Form von Handlungsanweisungen mit zahlreichen Abbildungen beschrieben.

Das Kompendium spiegelt geradlinig den empfohlenen Weg durch die Projektierung wieder, wobei zahlreiche Erfahrungen aus der Praxis ausgewertet werden. Die Beschreibung geht nicht bis in die Applikation selbst, sondern bezieht sich auf den Umgang mit dem Projekt und die Parametereinstellungen der enthaltenen Komponenten.

Weitere Unterstützung

Bei Fragen zur Nutzung der im Handbuch beschriebenen Produkte wenden Sie sich an Ihren Siemens-Ansprechpartner in den für Sie zuständigen Vertretungen und Geschäftsstellen.

Ihren Ansprechpartner finden Sie unter http://www.siemens.com/automation/partner.

Den Wegweiser zum Angebot an technischen Dokumentationen für die einzelnen SIMATIC Produkte und Systeme finden Sie unter http://www.siemens.de/simatic-tech-doku-portal.

Den Online-Katalog und das Online-Bestellsystem finden Sie unter http://mall.automation.siemens.com/.

Trainingscenter

Um Ihnen den Einstieg in das Prozessleitsystem SIMATIC PCS 7 zu erleichtern, bieten wir entsprechende Kurse an. Wenden Sie sich an Ihr regionales Trainingscenter oder an das zentrale Trainingscenter in D 90327 Nürnberg (http://www.sitrain.com).

Technical Support

Sie erreichen den Technical Support für alle Industry Automation and Drive Technology Produkte über das Web-Formular für den Support Request http://www.siemens.de/automation/support-request.

Weitere Informationen zu unserem Technical Support finden Sie im Internet unter http://support.automation.siemens.com/WW/view/de/16604318.

Industry Online Support im Internet

Zusätzlich zu unserem Dokumentationsangebot bieten wir Ihnen im Internet unser Know-how an (http://support.automation.siemens.com).

Dort finden Sie:

- eine Übersicht zu den wichtigsten technischen Informationen und Lösungen für PCS 7 erhalten Sie unter http://www.siemens.de/industry/onlinesupport/pcs7.
- den Newsletter, der Sie ständig mit den aktuellsten Informationen zu Ihren Produkten versorgt.
- die für Sie richtigen Dokumente über unsere Suchfunktion im Industry Online Support-Portal.
- ein Forum, in welchem Anwender und Spezialisten weltweit Erfahrungen austauschen.
- Ihren Ansprechpartner für Industry Automation and Drive Technology vor Ort.

Informationen über Vor-Ort Service, Reparaturen, Ersatzteile. Vieles mehr steht für Sie unter dem Begriff "Leistungen" bereit.

2 Security-Strategien

2.1 Allgemein

Das Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) unterstützt Anlagenbetreiber bei Sicherheitsgutachten, zur Bereitstellung zusätzlicher Abwehrmaßnahmen zum Schutz vor Computer- und Netzwerksicherheitrisiken. Das ICS-CERT empfiehlt:

- Minimierung der Netzwerkschwachstellen für alle Leitsystemgeräte. Wichtige Geräte sollten keinen direkten Zugangs ins Internet haben.
- Das Leitsystemnetzwerk und die Remote-Geräte hinter einer Firewall platzieren und vom Firmennetz isolieren.
- Wird Remote-Zugang benötigt, sind sichere Methoden, wie z. B. Virtual Private Networks (VPNs), zu nutzen. Beachten Sie, dass das VPN nur so sicher ist, wie die angebundenen Geräte.

2.2 Konzept der tiefgestaffelten Verteidigung – "Defense-in-Depth"

Das Konzept der tiefgestaffelten Verteidigung (Defense-in-Depth) ist eine Security-Strategie, bei der sich mehrere Schichten (Layer) der Verteidigung um das zu verteidigende System, in diesem Fall das Automatisierungssystem, platzieren ("Peel the onion").

Die Implementierung einer tiefgestaffelten Verteidigung bedarf einer Kombination aus unterschiedlichen Sicherheitsmaßnahmen. Dazu gehören:

- Physikalische Sicherheitsmaßnahmen:
  Kontrolle des physischen Zugangs zu räumlichen Bereichen, Gebäuden, einzelnen Räumen, Schränken, Geräten, Betriebsmitteln, Kabeln und Drähten. Die physikalischen Sicherheitsmaßnahmen müssen an den Security-Zellen und den verantwortlichen Personen ausgerichtet sein. Es ist wichtig, physischen Schutz auch an entfernten Einzelplatzsystemen zu realisieren.
- Organisatorische Sicherheitsmaßnahmen:
  Sicherheitsrichtlinien, Sicherheitskonzepte, Sicherheitsregelwerke, Security Checks, Risiko Analysen, Assessments und Audits, Awareness-Maßnahmen und Trainings.

Die physikalischen und organisatorischen Sicherheitsmaßnahmen werden unter der Überschrift "Plant Security" zusammengefasst.

- Aufteilung in Sicherheitszellen
  Eine umfassend abgesicherte Netzwerkarchitektur unterteilt das leittechnische Netzwerk in verschiedene Aufgabenebenen.
  Es sollen Perimeterzonen-Techniken eingesetzt werden. Das bedeutet in diesem Fall die Verwendung exportierter und nicht direkt der Prozesssteuerung dienender Daten, die auf einem System (Datenspeicher, Datenbank) verfügbar sind. Das System befindet sich zwischen dem Hauptzugriffspunkt für den Dateneingang (Frontend Firewall) und dem tief eingebetteten Zugriffspunkt für den Dateneingang (Backend Firewall) oder im dritten Netzwerkabschnitt einer Threehomed Firewall (in drei Netzwerken angesiedelt).
- Sicherung der Zugangspunkte zu den Sicherheitszellen
  Ein einziger Zugriffspunkt (Single Access Point) zu jeder Sicherheitszelle (soll eine Firewall sein) für die Authentifizierung von Benutzern, benutzten Geräten und Anwendungen, für die richtungsbasierte Zugriffssteuerung und die Vergabe von Zugriffsberechtigungen sowie für die Feststellung von Einbruchsversuchen.

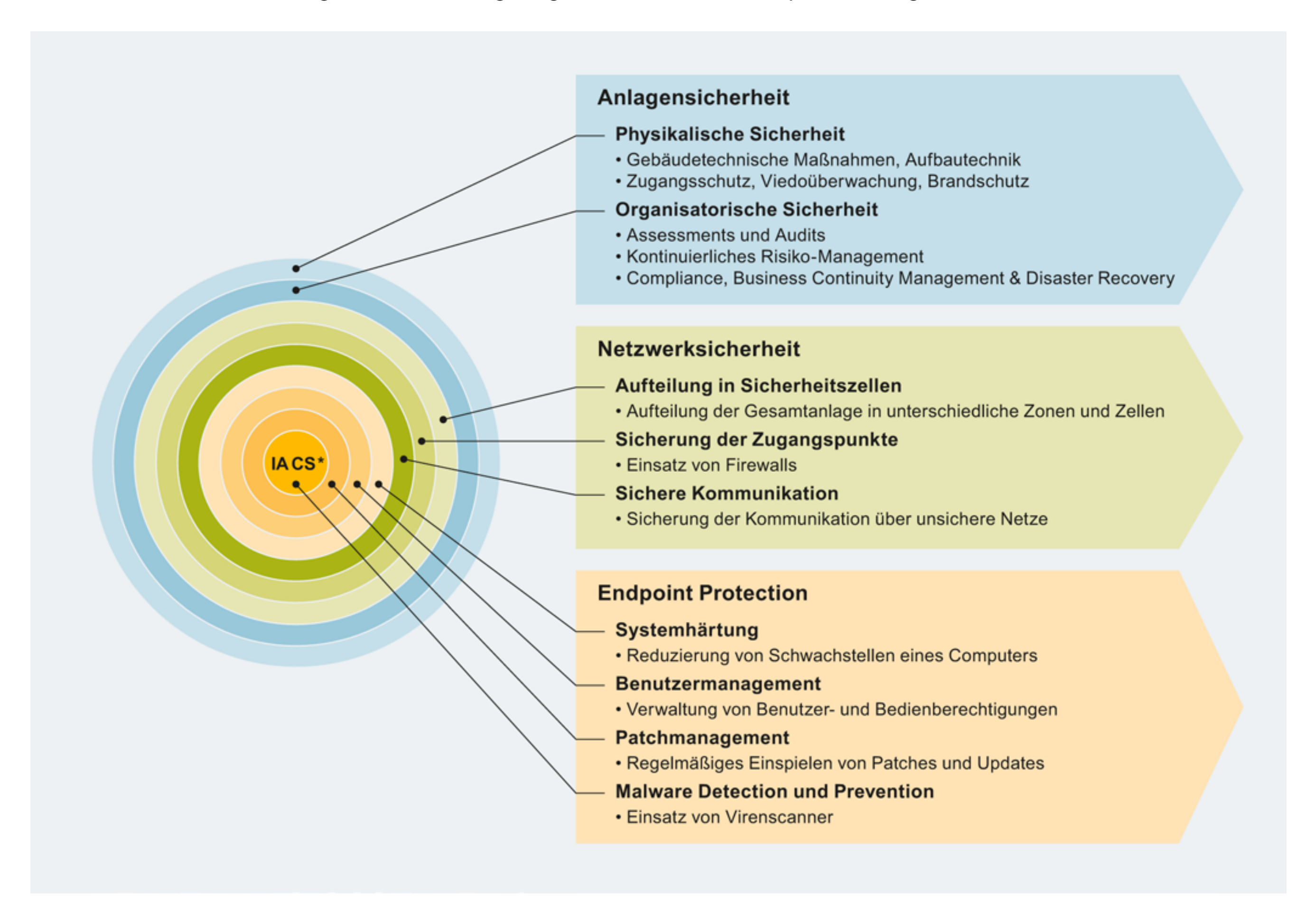
  Der Single Access Point fungiert als Haupteingangspunkt zum Netzwerk einer Sicherheitszelle und dient als erster Punkt einer Steuerung von Zugriffsrechten auf Netzwerkebene.
- Sicherung der Kommunikation zwischen zwei Sicherheitszellen über ein "unsicheres" Netzwerk
  Zertifikatsbasierte, authentifizierte und verschlüsselte Kommunikation soll immer dann eingesetzt werden, wenn die Perimeterzonen-Technik oder die Standard Application Layer Filtering-Technik nicht verfügbar sind. Dies kann mittels Tunnelprotokollen wie PPTP (Point To Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), IPSec- (IPSecurity-) Filterung oder auch über Kanäle geschehen, die durch serverbasierte Zertifikate abgesichert sind, wie z. B. RDP (Remote Desktop Protocol), einen über HTTPS sicher publizierten Windows Server-Terminal oder Windows Server-Web Server über die Firewall unter Verwendung der SSL-(Secure Sockets Layer-)Technologie.

Die Maßnahmen bezüglich der Sicherheitszellen, z. B. Bildung von Sicherheitszellen, Sicherung der Zugangspunkte und die sichere Kommunikation zwischen unterschiedlichen Sicherheitszellen, werden unter der Überschrift "Netzwerksicherheit" zusammengefasst.

- Systemhärtung
  Systemeinstellungen eines Computers, die ihn widerstandsfähiger gegen Angriffe durch Schadsoftware machen.
- Benutzermanagement und rollenbasierte Bedienberechtigungen
  Aufgabenbezogene Bedien- und Zugriffsrechte (role-based access control)
- Patchmanagement
  Patchmanagement ist die planmäßige Vorgehensweise zur Installation von Updates auf Anlagencomputern.
- Malware Detection & Prevention
  Einsatz von geeigneten und richtig konfigurierten Virenscannern

Die Maßnahmen "Systemhärtung", "Benutzer- und Patchmanagement" sowie "Malware Detection & Prevention" werden unter der Überschrift "Integrity Protection" oder "Endpoint Protection" zusammengefasst.

Die folgende Abbildung zeigt die "Defense-in-Depth" Strategie:



*IA CS: Industrial Automation Control System

2.3 Musterkonfiguration

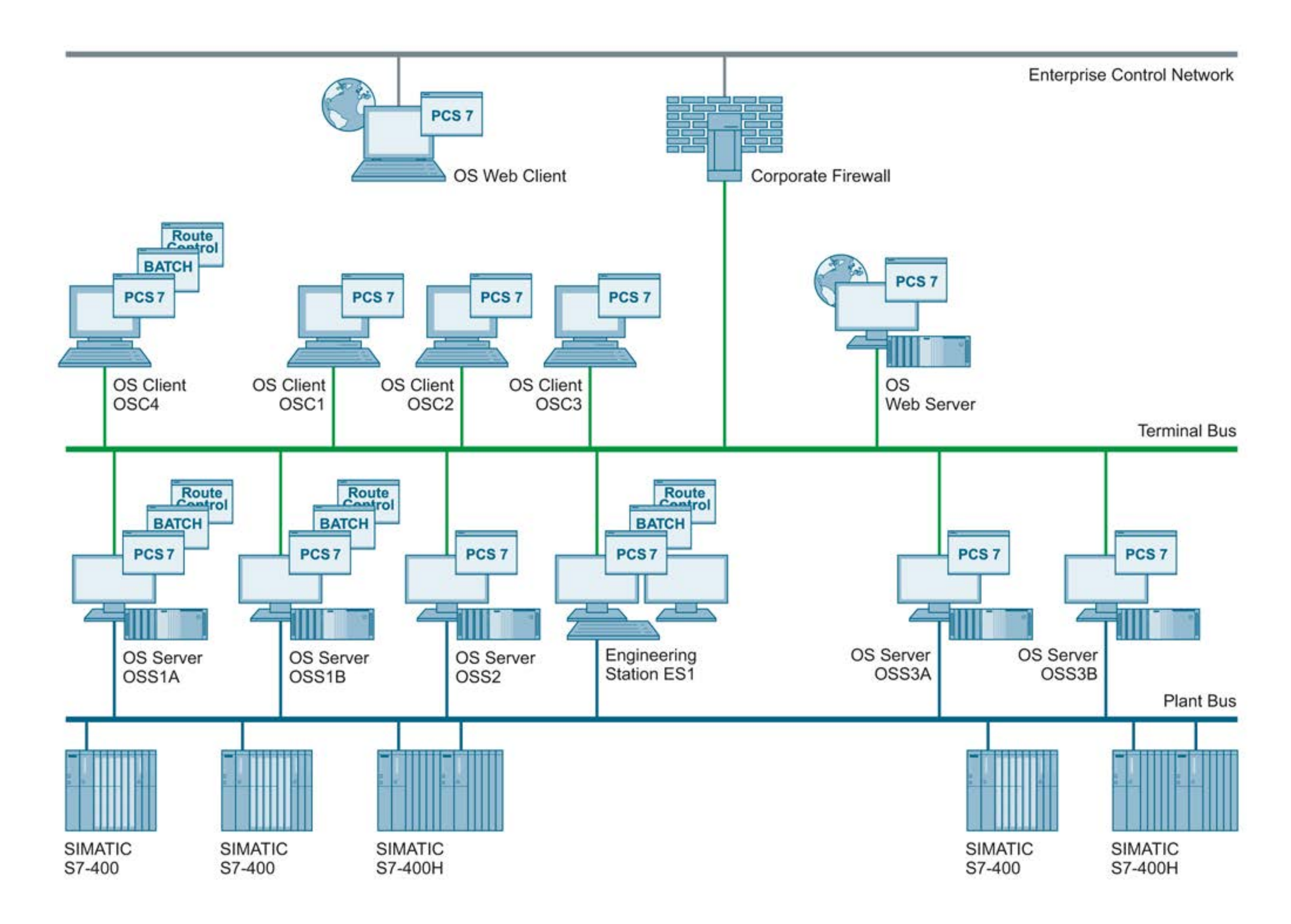
Dieses Kompendium orientiert sich in Aufbau und Struktur an dem Konzept der tiefgestaffelten Verteidigung. Die einzelnen Kapitel gliedern sich, entsprechend dem Konzept, in die Maßnahmen der Netzwerksicherheit (Einteilung in Sicherheitszellen, Sicherung der Zugangspunkte und die sichere Kommunikation zwischen Komponenten in unterschiedlichen Sicherheitszellen) und in die Maßnahmen der System Integrity. Dazu zählen die Kapitel "Systemhärtung", "Benutzerverwaltung & Bedienberechtigung", "Patchmanagement" und "Virenscanner".

Hinweis

Beachten Sie, dass die in diesem Kapitel vorgestellte Musterkonfiguration eine Anlagenkonfiguration ohne jegliche Sicherheitsmaßnahmen zeigt. Die Musterkonfiguration ist, so wie oben dargestellt, aus Sicherheitssicht ein Negativbeispiel. Im weiteren Verlauf dieses Dokumentes wird Schritt für Schritt dargestellt, wie diese Anlagenkonfiguration durch die Implementierung von Sicherheitsmaßnahmen "sicherer" gemacht werden kann.

Musterkonfiguration

Die in diesem Kompendium vorgestellten Maßnahmen und Konfigurationsbeispiele werden anhand der folgenden Musterkonfiguration erläutert:



Die Musterkonfiguration besteht aus insgesamt fünf S7-Steuerungen, die die Mess-, Steuerungs- und Regelungsaufgaben innerhalb der verfahrenstechnischen Anlage übernehmen. Zur Bedienung und Beobachtung sind fünf OS-Server (zwei redundante Serverpaare sowie ein einzelner OS-Server) sowie vier OS-Clients vorgesehen. Des Weiteren ist ein Web Server zur Bedienung und Beobachtung über das Corporate-Netzwerk und das Internet vorgesehen. Dazu ist der Terminalbus mit dem Corporate-Netzwerk verbunden, das wiederum einen Internetzugang zur Verfügung stellt. Für die Projektierung der Gesamtanlage ist eine Engineering Station vorhanden.

Die verfahrenstechnische Anlage teilt sich in zwei mehr oder weniger unabhängige Teilanlagen. Für die Mess-, Steuerungs- und Regelungsaufgaben der Teilanlage A werden drei S7-Steuerungen, für die der Teilanlage B insgesamt zwei S7-Steuerungen eingesetzt. Über die vier OS-Clients sollen eine Bedienung und Beobachtung beider Teilanlagen möglich sein. Dabei sind der Teilanlage A und B je ein redundantes OS-Serverpaar zugeordnet. Die Teilanlage A hat zusätzlich noch einen weiteren OS-Server, der allerdings nicht redundant ausgeführt ist. Ein OS-Client soll als Vor-Ort-Bedienstation einer Abfüllstation dienen.

Netzwerksicherheit 3

3.1 Automatisierungs- und Sicherheitszellen

Die Strategie der Aufteilung von Anlagen und verbundenen Anlagen in Sicherheitszellen erhöht die Verfügbarkeit eines Gesamtsystems. Einzelne Ausfälle oder Sicherheitsbedrohungen, die Ausfälle hervorrufen, lassen sich damit auf ihren unmittelbaren Wirkungskreis begrenzen. Bei der Planung der Sicherheitszellen wird die Anlage zuerst in Automatisierungszellen (process cells) und anschließend durch Security-Maßnahmen in Sicherheitszellen (security cells) unterteilt.

Kriterien zur Aufteilung einer Anlage in Automatisierungs- und Sicherheitszellen finden Sie in den folgenden Dokumenten:

- Sicherheitskonzept PCS 7 & WinCC (Basis) (http://support.automation.siemens.com/WW/view/de/60119725)
- Sicherheitskonzept PCS 7 Empfehlungen und Hinweise (http://support.automation.siemens.com/WW/view/de/22229786)

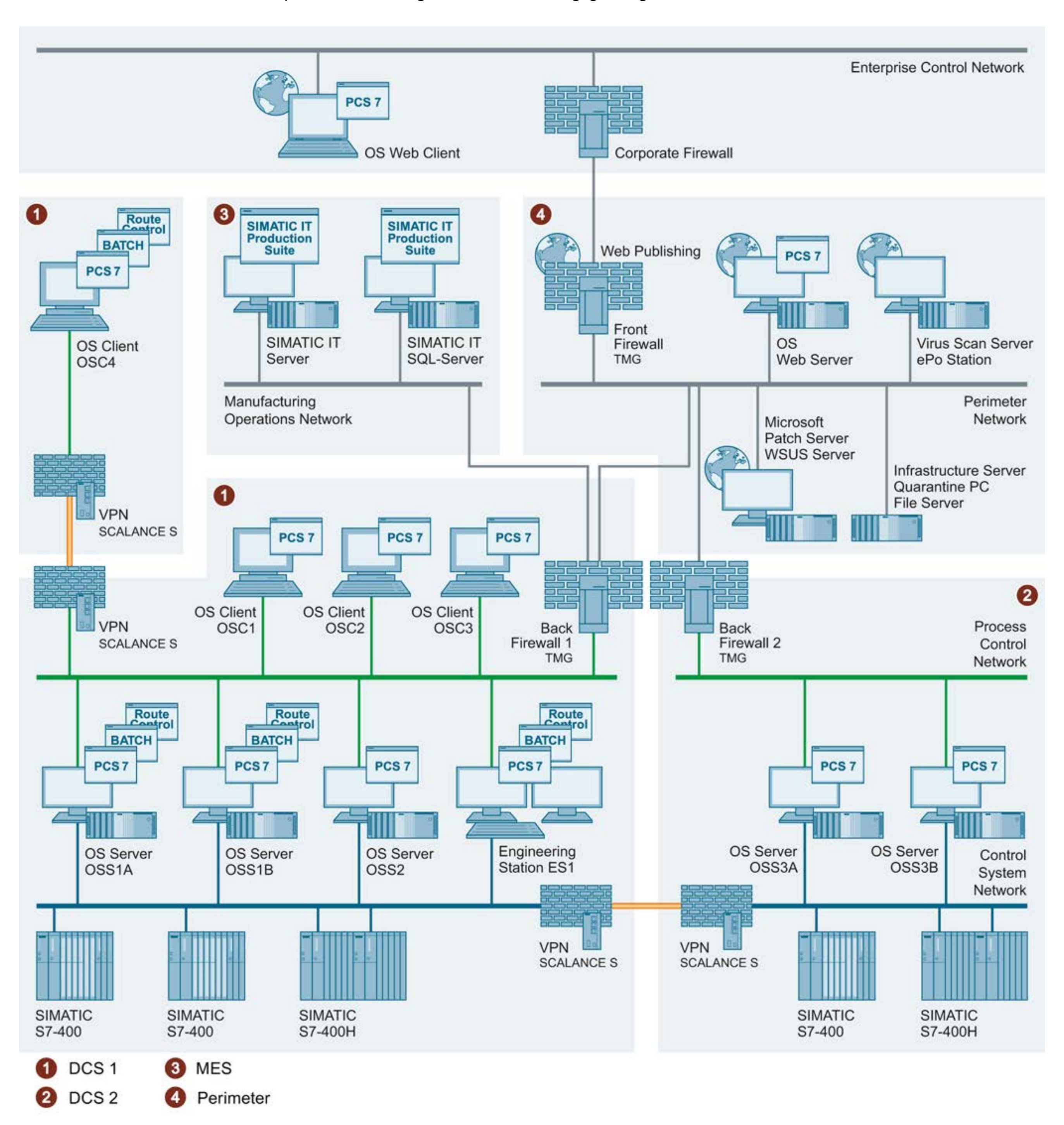
Musterkonfiguration: Aufteilung in Sicherheitszellen

Die Musterkonfiguration besteht aus zwei unabhängigen Teilanlagen mit einer gemeinsamen Bedien- und Beobachtungsebene. Somit kann eine Sicherheitszelle für die Teilanlage A mit den jeweils der Teilanlage A zugeordneten S7-Steuerungen und OS-Servern gebildet werden. Für die Teilanlage B und den dieser Teilanlage zugeordneten Steuerungen und OS-Servern wird eine separate Sicherheitszelle gebildet.

Die Aufteilung der Gesamtanlage in eine Sicherheitszelle für die Teilanlage A sowie für die Teilanlage B bedingt auch die Auftrennung von Anlagen- und Terminalbus. Die OS-Clients, auf denen eine Bedienung und Beobachtung des Gesamtprozesses (Teilanlage A und B) möglich sein soll, werden der Sicherheitszelle der Teilanlage A zugeordnet. Somit muss eine Kommunikation zwischen den Sicherheitszellen von Teilanlage A und B sichergestellt werden.

Der Web Server, der zur Bedienung und Beobachtung aus dem Corporate-Netzwerk bzw. aus dem Internet dient, wird in einer separaten Sicherheitszelle (Perimeter) platziert. In dieser Sicherheitszelle werden auch Virenscan-Server und WSUS-Update-Server platziert. Für einen Datenaustausch (Projektdaten/Projektbackup) zwischen den Sicherheitszellen wird auch ein Quarantäne-PC in der Perimeter-Sicherheitszelle implementiert.

Die Komponenten der Produktionsplanungsanbindung (SIMATIC IT) werden wiederum in einer separaten Sicherheitszelle (MES) zusammengefasst. Somit ergeben sich für die Musterkonfiguration insgesamt vier verschiedene Sicherheitszellen (DCS1, DCS2, MES und Perimeter), die in der folgenden Abbildung gezeigt sind:



3.2 Adressierung und Segmentierung

IP-Adresse

Hinweis

Der Begriff "IP-Adresse" wird in diesem Dokument mit der Bedeutung von IPv4-Adresse verwendet. Dem gegenüber steht eine IPv6-Adresse. Auf die IPv6-Adresse wird in diesem Dokument nicht eingegangen

Quelle: http://www.microsoft.com/germany/technet/datenbank/articles/600667.mspx?pf=true

Eine IP-Adresse besteht aus 32 Bit. Üblicherweise wird eine Notation verwendet, bei der jeweils vier Dezimalzahlen (zwischen 0 bis 255) durch Punkte voneinander getrennt werden (Punkt-Dezimalnotation). Jede Dezimalzahl, auch als Oktett bekannt, stellt 8 Bit (1 Byte) der aus 32-Bit bestehenden Adresse dar:

IPv4-Adresse				
Binär	1100 0000	1010 1000	0000 0001	0000 1010
Hexadezimal	C 0	A 8	0 1	0 A
Dezimal	192	168	1	10

Subnetzwerke

Die Strategie einer räumlichen und funktionalen Aufteilung einer Automatisierungsanlage muss sich auch bei der Netzwerkkonfiguration widerspiegeln. Dies kann durch die Wahl des IP-Adressbereichs und die damit verbundene Bildung von Subnetzen erreicht werden. Subnetze dienen dazu, ein bestehendes Netz in weitere, kleinere Netze (PCN, CSN, MON, Perimeter) zu unterteilen ohne dafür zusätzliche Klasse-A, Klasse-B oder Klasse-C IP-Adressen zu benötigen.
Als Subnetz wird somit ein Teilnetz eines Netzwerks beim Internetprotokoll (IP) bezeichnet. Das Subnetz fasst mehrere aufeinanderfolgende IP-Adressen mittels einer Subnetzmaske zusammen. Somit teilt die Subnetzmaske eine IP-Adresse in einen Netzwerk-Teil und einen Host-Teil auf. Sie hat denselben Aufbau wie eine IP-Adresse (4 Byte). Per Definition sind alle Bits des Netzwerk-Teils auf TRUE = 1 und alle Bits des Host-Teils auf FALSE = 0 zu setzen.

Netzwerk- und Host Teil einer IP-Adresse					
IP-Adresse	141.84.65.2	1000 1101	0101 0100	0110 0101	0000 0010
Netzmaske	255.255.255.0	1111 1111	1111 1111	1111 1111	0000 0000
Netzwerk	141.84.65.0	1000 1101	0101 0100	0110 0101	0000 0000
		0000 0000	0000 0000	0000 0000	1111 1111
Host	2	0000 0000	0000 0000	0000 0000	0000 0010

Netzwerkklassen

Quelle: http://www.microsoft.com/germany/technet/datenbank/articles/600667.mspx?pf=true

Die Adressklassen wurden von Internet Assigned Numbers Authority (IANA) definiert, um Adresspräfixe systematisch zu Netzwerken mit variierender Größe zuzuordnen. Die Klasse der Adressen gibt an, wie viele Bits für die Netzwerk-ID und wie viele Bits für die Host-ID verwendet wurden. Durch die Adressklassen wurden außerdem die mögliche Anzahl von Netzwerken sowie die Anzahl der Hosts pro Netzwerk festgelegt. Von den fünf Adressklassen waren die Klasse A, B und C für IPv4-Unicast-Adressen reserviert. Innerhalb dieser drei Netzwerkklassen wurden auch private IP-Adressbereiche festgelegt. Diese privaten IP-Adressbereiche haben aus der Sicht der Netzwerksicherheit den Vorteil, dass sie nicht im Internet weitergeleitet (geroutet) werden können. Damit wird bereits ein direkter Angriff aus dem Internet auf einen Anlagen-PC verhindert.

Netzadressenbereich	CIDR-Notation	Anzahl der Adressen	Netzklasse
10.0.0.0 – 10.255.255.255	10.0.0.0/8	224 = 16.777.216	Klasse A: 1 privates Netz mit 16.777.216 Adressen
172.16.0.0 – 172.31.255.255	172.16.0.0/12	220 = 1.048.576	Klasse B: 16 private Netze mit je 65.536 Adressen
192.168.0.0 – 192.168.255.255	192.168.0.0/16	216 = 65.536	Klasse C: 256 private Netze mit je 256 Adressen

3.2.1 Musterkonfiguration: Aufteilung in Subnetze

Für die Adressierung der Automatisierungsnetzwerke in der Musterkonfiguration (Anlagenbus CSN, Terminalbus PCN, usw.) sollen Adressen aus dem privaten IP-Adressbereich für Klasse C verwendet werden. In diesem Bereich gibt es

- 256 Klasse C Netzwerke (Subnet 192.168.0.x bis 192.168.255.x)
- 254 Hosts pro Netzwerk (IPv4-Adresse 192.168.x.1 bis 192.168.x.254)

Die Netzadresse 192.168.2.0 muss in vier gleich große Subnetze (gleiche Anzahl an Hosts im Subnetz) geteilt werden. Für die Aufteilung in vier Netze (Perimeter-Netzwerk, Process Control-Netzwerk 1, Process Control-Netzwerk 2 und Manufacturing Operations-Netzwerk) werden 2 Bits benötigt ($2^2 = 4$).

Somit kann die Segmentierung in vier Netze mit der folgenden Subnetzmaske erreicht werden:

```
1111 1111.1111 1111.1111 1111.1100 0000 = 255.255.255.192
```

Daraus ergeben sich die folgenden Netze:

- Netz 1: Manufacturing Operations-Netzwerk (IP-Adressen des MON)

Netz 1: Manufacturing Operations-Netzwerk	
Netzwerk-Adresse	192.168.2.0
Adresse des ersten Hosts	192.168.2.1
Adresse des letzten Hosts	192.168.2.62
Broadcast-Adresse	192.168.2.63

- Netz 2: Process Control-Netzwerk 1 (IP-Adressen des PCN1 (Teilanlage A))

Netz 2: Process Control-Netzwerk 1	
Netzwerk-Adresse	192.168.2.64
Adresse des ersten Hosts	192.168.2.65
Adresse des letzten Hosts	192.168.2.126
Broadcast-Adresse	192.168.2.127

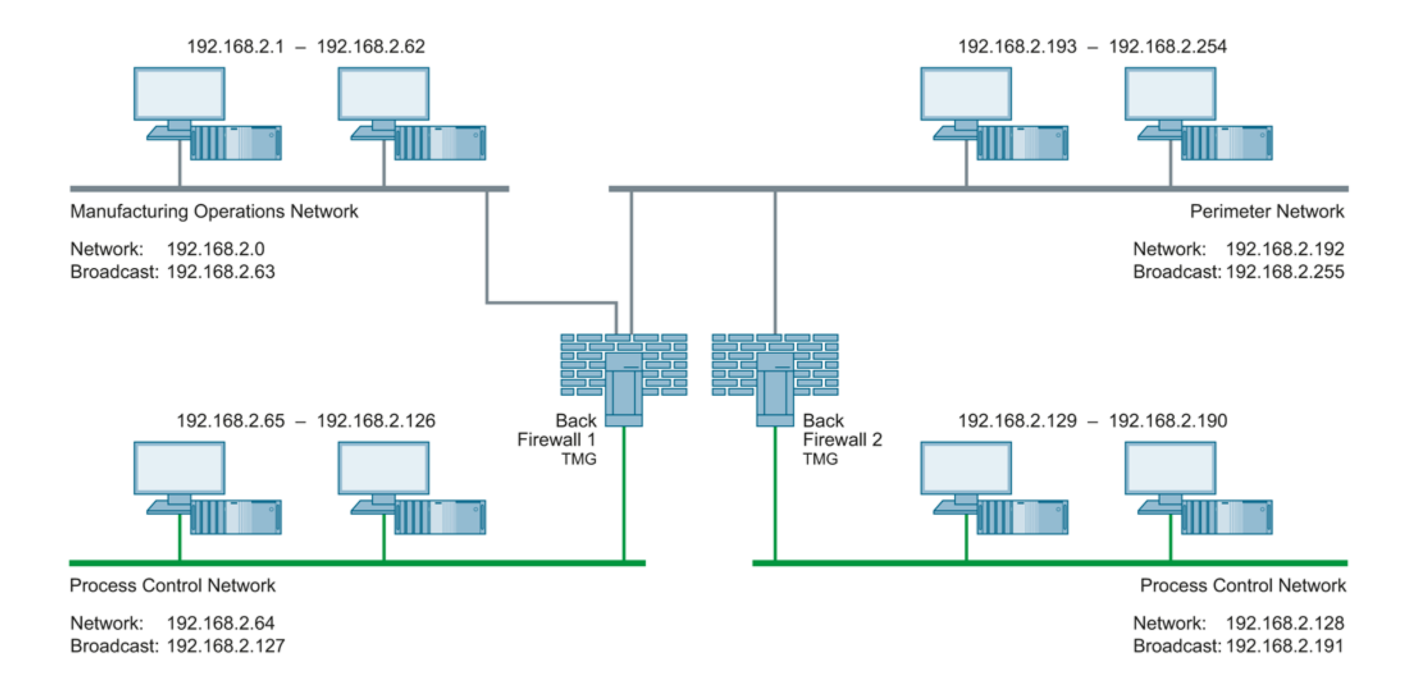
- Netz 3: Process Control-Netzwerk 2 (IP-Adressen des PCN2 (Teilanlage B))

Netz 3: Process Control-Netzwerk 2	
Netzwerk-Adresse	192.168.2.128
Adresse des ersten Hosts	192.168.2.129
Adresse des letzten Hosts	192.168.2.190
Broadcast-Adresse	192.168.2.191

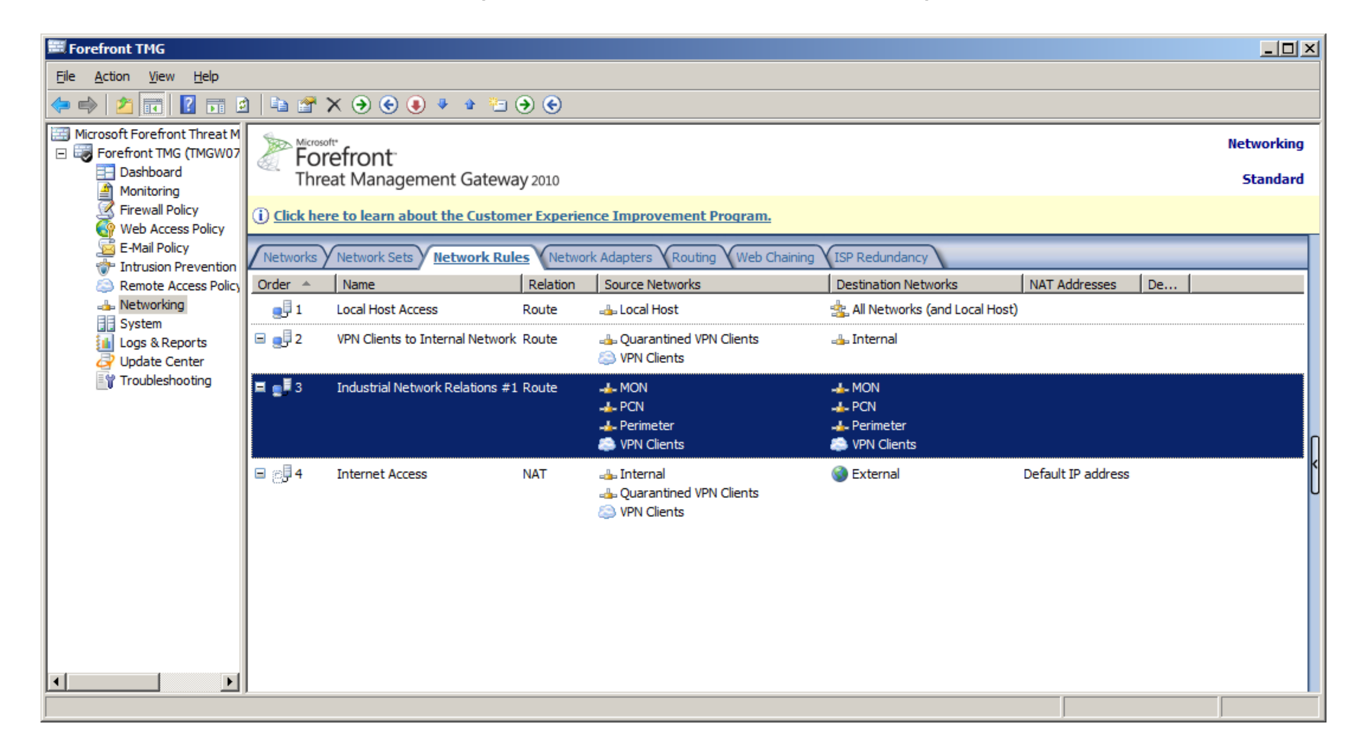
- Netz 4: Perimeter-Netzwerk (IP-Adresse des Perimeter-Netzwerks)

Netz 4: Perimeter-Netzwerk	
Netzwerk-Adresse	192.168.2.192
Adresse des ersten Hosts	192.168.2.193
Adresse des letzten Hosts	192.168.2.254
Broadcast-Adresse	192.168.2.255

Beispiel: Die vier Rechner mit den IP-Adressen 192.168.2.10, 192.168.2.100, 192.168.2.149 und 192.168.2.201 befinden sich in unterschiedlichen Subnetzen, zwischen denen kommuniziert werden muss. Broadcast-Adressen im Manufacturing Operations-Netzwerk werden somit nicht in die anderen Subnetze übertragen. Störungen in einzelnen Subnetzen bleiben lokal auf diese beschränkt.



Das Routing zwischen den unterschiedlichen Netzwerken übernehmen, in der o.g. Konfiguration die zwei Back Firewalls. Dazu ist die Erstellung einer entsprechenden Netzwerk-Regel innerhalb der verwendeten Firewall erforderlich. Das folgende Bild zeigt beispielhaft diese Regel im Microsoft Forefront TMG Management:



Diese Netzwerk-Regel übernimmt das Routing zwischen den PCN, MON und Perimeter-Netzwerken der Musterkonfiguration. Der Datenverkehr zwischen den Sicherheitszellen der Teilanlage A und B wird über beide Back Firewalls kommuniziert.

3.2.2 Musterkonfiguration: Einstellung der IP-Adressen und der Subnetzmaske

Vorgehensweise

Die folgende Vorgehensweise wird am Beispiel des Betriebssystems "Windows 7" beschrieben.

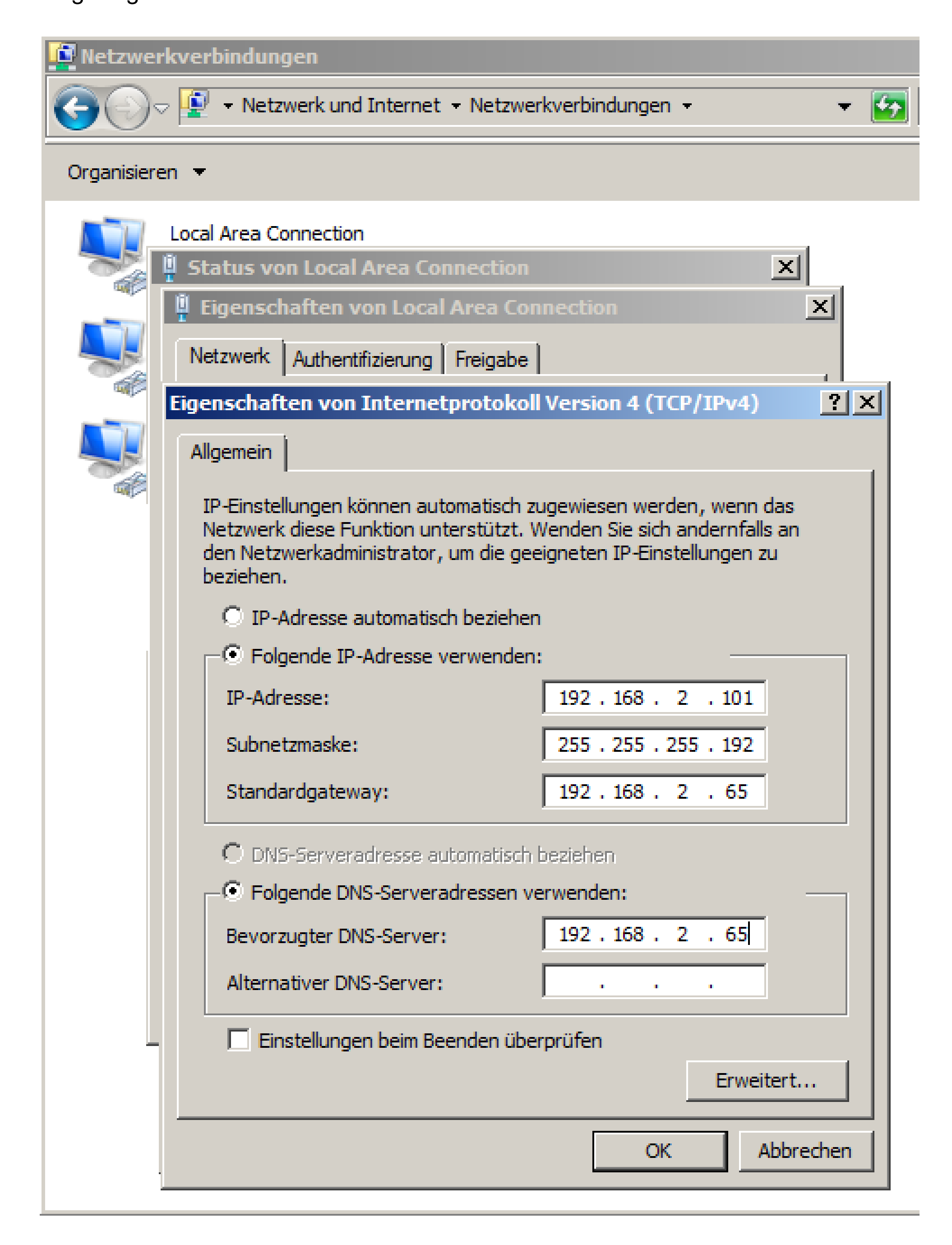
Um die IP-Adresse, die Subnetzmaske sowie das Standard-Gateway einzustellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Netzwerk- und Freigabecenter über den Befehl "Start > Systemsteuerung > Netzwerk- und Freigabecenter".
   Der Dialog "Netzwerk- und Freigabecenter" wird geöffnet.
2. Klicken Sie im linken Navigationsbereich des Dialogs auf den Eintrag "Adaptereinstellungen ändern".
   Der Dialog "Netzwerkverbindungen" wird geöffnet.
3. Öffnen Sie die Statusanzeige der entsprechenden Netzwerkverbindung (Process Control-Netzwerk 1 oder 2, Perimeter-Netzwerk oder Manufacturing Operations-Netzwerk) durch einen Doppelklick auf das entsprechende Symbol.
   Die Statusanzeige der Netzwerkverbindung wird geöffnet.
4. Klicken Sie auf die Schaltfläche "Eigenschaften".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Eigenschaftsdialog der ausgewählten Netzverbindung wird geöffnet.
5. Wählen Sie das Element "Internet Protocol Version 4(TCP/IPv4)" an und klicken auf die Schaltfläche "Eigenschaften".
   Der Eigenschaftendialog des Elements "Internet Protocol Version 4(TCP/IPv4)" wird geöffnet.
6. Wählen Sie die Option "Folgende IP-Adresse verwenden" aus und geben Sie im Feld "IP-Adresse" die IP Adresse des entsprechenden Computers an.
7. Geben Sie im Feld "Subnetzmaske" die Subnetzmaske des Computers ein.
8. Bestätigen Sie die Änderungen mit der Schaltfläche "OK".

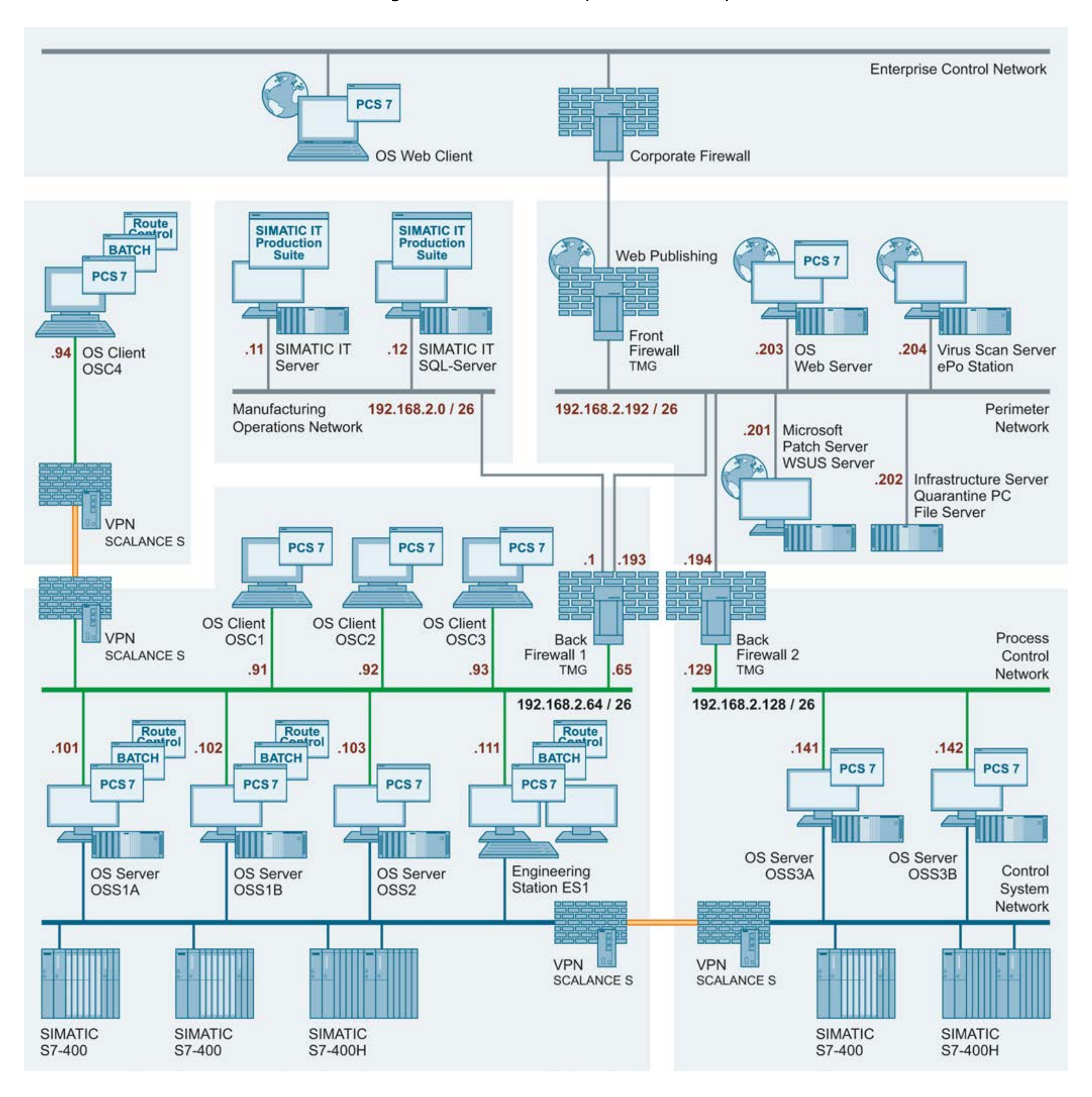
Beispiel

In der folgenden Abbildung wird ein Rechner adressiert, der sich im Process Control-Netzwerk 1 befindet. Der OS-Server mit dem Namen "OSS1A" hat eine Netzwerkverbindung zum Process Control-Netzwerk 1. Durch die Aufteilung in Subnetze wurde für dieses Netzwerk die Subnetzmaske 255.255.255.192 festgelegt. Als IP-Adressen innerhalb dieses Netzwerks stehen somit die Adressen von 192.168.2.65 bis 192.168.2.126 zur Verfügung.

Für den OS-Server "OSS1A" wurde die IP-Adresse 192.168.2.101 festgelegt und in das Feld "IP-Adresse" des Eigenschaftendialogs "Internet Protocol Version 4(TCP/IPv4)" eingefügt. In das Feld "Subnetzmaske" wurde die oben festgelegte Subnetzmaske 255.255.255.192 eingetragen.



Auf diese Weise vergeben Sie allen Computern die entsprechende IP-Adresse.



3.3 Namensauflösung

Rechnernamen

Durch den Rechnername kann ein Rechner innerhalb eines Netzwerkes eindeutig identifiziert werden. Dies ist die Voraussetzung, um mit dem Rechner zu kommunizieren. Der Name muss dabei eindeutig mit dem Rechner verbunden sein. Dadurch kann sichergestellt werden, dass ein Rechner zuverlässig gefunden wird. Eine versehentliche Doppelvergabe von Rechnernamen kann zu unvorhersehbaren Verhalten während der Kommunikation führen.
Da der NetBIOS-Name vom Rechnername abgeleitet wird (siehe NetBIOS-Name) und zur NetBIOS-Namensauflösung der NetBIOS-Name eindeutig sein muss, darf der Rechnername nicht länger als 15 Zeichen sein.
Der Rechnername muss eindeutig sein und soll einen Rückschluss auf die Funktion des Rechners zulassen.

Hinweis

Die Regeln zur Vergabe des Rechnernamens entnehmen Sie dem Installationshandbuch "SIMATIC Prozessleitsystem PCS 7 PC-Konfiguration und Autorisierung" (http://support.automation.siemens.com/WW/view/de/68157327).

Beachten Sie auch die folgenden Dokumenten:

- FAQ "Warum ist in PCS 7 der Unterstrich als Zeichen beim Rechnernamen nicht erlaubt?" (http://support.automation.siemens.com/WW/view/de/67794552)
- Microsoft Support Center: "Namenskonventionen in Active Directory für Computer, Domänen, Standorte und Organisationseinheiten" (http://support.microsoft.com/kb/909264/de)

Weitere Namenskonventionen finden Sie in den folgenden Dokumenten:

- Handbuch "SIMATIC Prozessleitsystem PCS 7 Engineering System" (http://support.automation.siemens.com/WW/view/de/68157345), Abschnitt "Regeln für die Namensgebung der TH"
- Online-Hilfe WinCC Informationssystem "Arbeiten mit Projekten > Anhang > Nicht erlaubte Zeichen"
- Datei "Projects.pdf". Diese Datei finden Sie im Installationsorder der SIMATIC Produktreihe der SIEMENS AG

Ändern des Rechnernamens

ACHTUNG
Der Rechnername darf nur vor der Installation von SIMATIC PCS 7 und vor dem ersten Öffnen des WinCC-Explorer geändert werden.

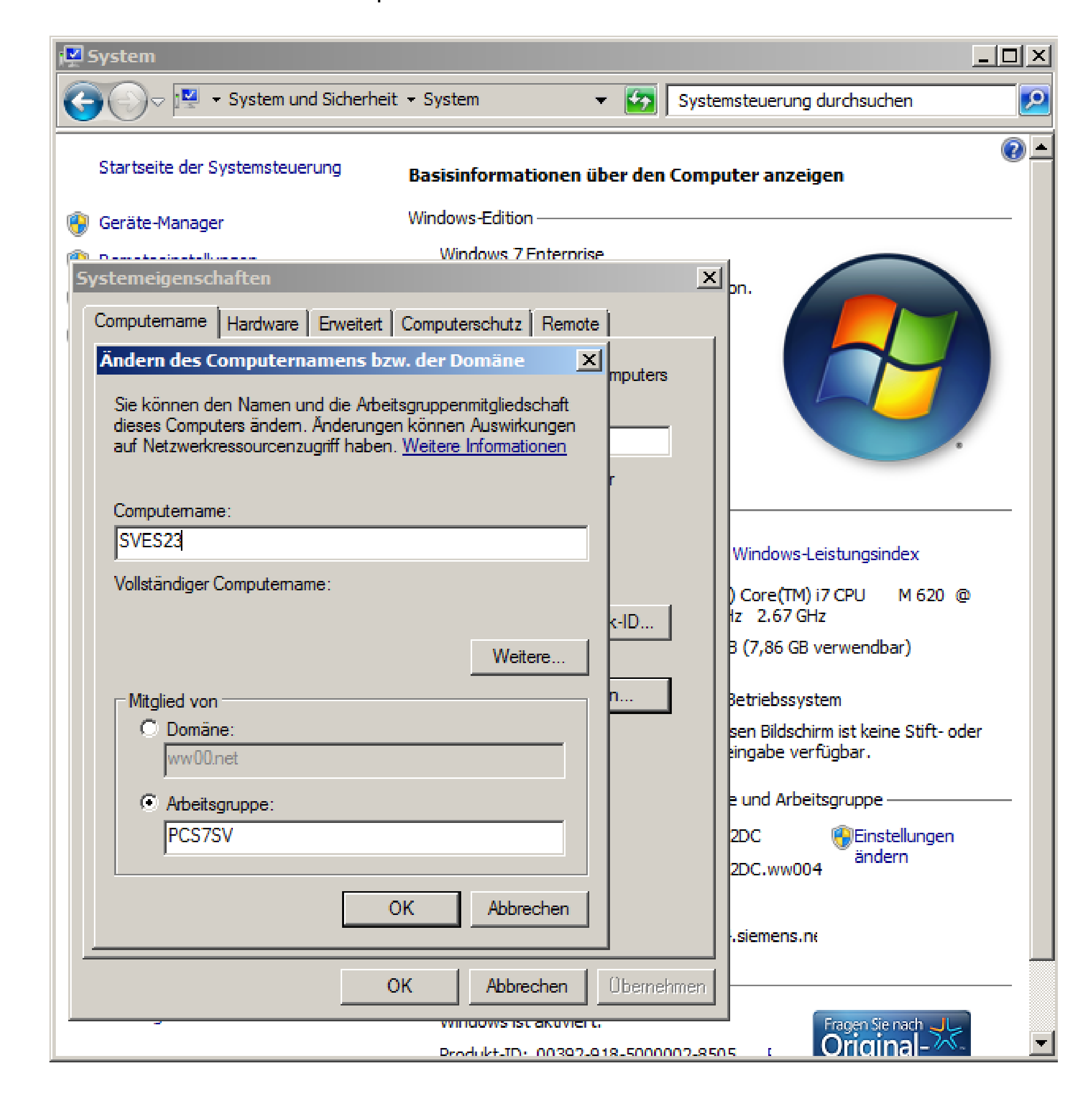
Vorgehensweise

Die folgende Vorgehensweise wird am Beispiel des Betriebssystems "Windows 7" beschrieben.

Um den Rechnernamen zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie den Befehl "Start > Systemsteuerung (Control Panel) > System und Sicherheit (System)".
   Der Dialog "System" wird geöffnet.
2. Klicken Sie im Bereich "Einstellungen für Rechnernamen, Domäne und Arbeitsgruppe" auf den Link "Einstellungen ändern".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie bereits als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Dialog "Systemeigenschaften" wird geöffnet.
3. Klicken Sie im Register "Computername" auf die Schaltfläche "Ändern".
   Der Dialog "Ändern des Computernamens bzw. der Domäne" wird geöffnet.

4. Geben Sie im Feld "Computername" den Namen des Rechners ein.



NetBIOS-Name

Quelle: Microsoft Support Center "TCP/IP-Grundlagen für Microsoft Windows"

Ein NetBIOS-Name ist ein 16 Byte (16 Zeichen) langer Name, auf der Basis des Rechnernamens, der eine NetBIOS-Anwendung im Netzwerk bezeichnet. Als exakten Namen verwendet der Dienst die ersten 15 Zeichen des Rechnernamens zuzüglich des Zeichens 0x20 als 16tes Zeichen. Ein NetBIOS-Name ist entweder ein eindeutiger (exklusiver) Name oder ein (nicht exklusiver) Gruppenname. Wenn eine NetBIOS-Anwendung mit einer bestimmten NetBIOS-Anwendung auf einem einzelnen Rechner kommuniziert, werden eindeutige Namen verwendet. Wenn ein NetBIOS-Prozess mit mehreren NetBIOS-Anwendungen auf verschiedenen Rechnern kommuniziert, wird ein Gruppenname verwendet.

Fully Qualified Domain Name

Der "Fully Qualified Domain Name" (FQDN) setzt sich aus dem Rechnernamen und dem Domain-Namen zusammen und kann damit nicht mehrfach verwendet werden.

NetBIOS-Namensauflösung

Quelle: Microsoft Support Center "TCP/IP-Grundlagen für Microsoft Windows"

Unter NetBIOS-Namensauflösung versteht man den Vorgang der Zuordnung einer IPv4-Adresse zu einem NetBIOS-Namen. Für die erfolgreiche NetBIOS-Namensauflösung können folgende Methoden angewendet werden:

- Standardmethoden zur NetBIOS-Namensauflösung

Methode	Beschreibung
NetBIOS Name Cache	Eine im RAM gespeicherte lokale Tabelle, die die vom lokalen Rechner vor kurzem aufgelösten NetBIOS-Namen mit den zugehörigen IPv4-Adressen enthält.
NBNS	Ein Server, der die NetBIOS-Namen bereitstellt. Bei WINS handelt es sich um die Microsoft-Implementierung eines NBNS.
Lokaler Broadcast	NetBIOS Name Query Request Broadcast-Nachrichten, die an das lokale Subnetz gesendet werden.

- Zusätzliche Microsoft-spezifische Methoden zur NetBIOS-Namensauflösung

Methode	Beschreibung
Lmhosts-Dateien	Lokale Textdatei, in der NetBIOS-Namen ihren IPv4-Adressen zugeordnet werden. Die Lmhosts-Datei wird für NetBIOS-Anwendungen verwendet, die auf Rechnern in Remote-Subnetzen ausgeführt werden.
Lokaler Host-Name	Konfigurierter Host-Name des Rechners
DNS-Auflösungscache	Lokale RAM-basierte Tabelle, die die Domain-Namen- und IPv4-Adressenzuordnungen aus der lokalen HOSTS-Datei enthält sowie die Namen, die über DNS aufgelöst werden sollen.
DNS-Server	Server, der die Datenbanken mit Zuordnungen von IPv4-Adressen zu Host-Namen verwalten.

NetBIOS-Namensauflösung mittels Verwendung der Lmhosts-Datei

Quelle: Microsoft Support Center "TCP/IP-Grundlagen für Microsoft Windows"

Bei der Lmhosts-Datei handelt es sich um eine statische Textdatei mit NetBIOS-Namen und IPv4-Adressen. NetBT verwendet die Lmhosts-Datei, um NetBIOS-Namen für NetBIOS-Anwendungen aufzulösen, die auf Remote-Rechnern in einem Netzwerk ohne NBNS ausgeführt werden. Die Lmhosts-Datei weist folgende Merkmale auf:

- Einträge bestehen aus einer IPv4-Adresse und einem NetBIOS-Rechnernamen wie z. B.:

  ```
  131.107.7.29 OSSRV01
  ```

- Bei den Einträgen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Auf jedem Rechner befindet sich jeweils eine eigene Datei im Ordner %windir%\system32\Drivers\etc

Dieser Ordner enthält auch eine Lmhosts-Beispieldatei (Lmhosts.sam). Sie können eine eigene Datei mit dem Namen Lmhosts erstellen oder Lmhosts.sam aus diesem Ordner nach Lmhosts kopieren.

Um die Netzwerk-Broadcasts zu vermeiden, sollen die Einträge in der Lmhosts-Datei mit dem Schlüsselwort #PRE erfolgen. Das Schlüsselwort #PRE legt fest, welche Einträge bereits zu Anfang als permanente Einträge in den NetBIOS Name Cache geladen werden sollen. Durch vorher geladene Einträge werden die Netzwerk-Broadcasts reduziert, da Namen ggf. über den Cache anstatt durch Broadcast-Abfragen aufgelöst werden können.

Beispiel:

```
192.168.2.101 OSSRV01A    #PRE
192.168.2.102 OSSRV01B    #PRE
```

NetBIOS-Namensauflösung mit NetBIOS-Namenserver

Quelle: Microsoft Support Center "TCP/IP-Grundlagen für Microsoft Windows"

Um NetBIOS-Namen von NetBIOS-Anwendungen aufzulösen, die auf lokalen Rechnern oder auf Remotecomputern ausgeführt werden, wird bei NetBT normalerweise ein NetBIOS-Name Server (NBNS) verwendet. Wenn ein NBNS verwendet wird, erfolgt die Namensauflösung wie folgt:

1. NetBT überprüft den NetBIOS Name Cache auf Zuordnungen von NetBIOS-Namen zu IPv4-Adressen.
2. Wenn der Name mit dem NetBIOS Name Cache nicht aufgelöst werden kann, sendet NetBT eine NetBIOS Name Query Request Unicast -Nachricht an den NBNS, die den NetBIOS-Namen der Zielanwendung enthält.
3. Wenn der NBNS den NetBIOS-Namen zu einer IPv4-Adresse auflösen kann, gibt der NBNS die IPv4-Adresse an den sendenden Host mit einer positiven NetBIOS Name Query Response-Nachricht zurück. Wenn der NBNS den NetBIOS-Namen nicht zu einer IPv4-Adresse auflösen kann, sendet der NBNS eine negative NetBIOS Name Query Response-Nachricht.

Auf einem Rechner unter Windows Server 2003 oder Windows XP wird dreimal versucht, den primären NBNS-Server zu finden. Wenn keine Antwort empfangen wird oder eine negative NetBIOS Name Query Response-Nachricht das Fehlschlagen der Namensauflösung anzeigt, versucht ein Rechner unter Windows zusätzliche WINS-Server zu kontaktieren.

WINS (Windows Internet Name Service) ist die Windows-Implementierung eines NetBIOS Name Servers (NBNS), der eine verteilte Datenbank für das Registrieren und Abfragen dynamischer Zuordnungen von NetBIOS-Namen zu den im Netzwerk verwendeten IPv4-Adressen bereitstellt.

Host-Namensauflösung (DNS-Namensauflösung)

Quelle: Microsoft Support Center "TCP/IP-Grundlagen für Microsoft Windows"

Mit Host-Namensauflösung ist die richtige Zuordnung eines Host-Namens zu einer IP-Adresse gemeint. Bei einem Host-Namen handelt es sich um einen Aliasnamen, der einem IP-Knoten zugewiesen wurde. Der IP-Knoten ist somit als TCP/IP-Host gekennzeichnet. Der Host-Name kann aus bis zu 255 Zeichen bestehen. Er kann alphabetische und numerische Zeichen, Bindestriche und Punkte enthalten. Sie können demselben Host mehrere Host-Namen zuordnen.

Bei Winsock-Programmen (Windows Sockets), z. B. Internet Explorer und dem Dienstprogramm FTP, kann für das gewünschte Ziel der Verbindung einer von zwei Werten eingesetzt werden: die IP-Adresse oder ein Host-Name. Wenn die IP-Adresse angegeben wird, ist die Namensauflösung nicht erforderlich. Wird ein Host-Name angegeben, muss dieser in eine IP-Adresse aufgelöst werden, bevor die IP-Kommunikation mit der gewünschten Ressource beginnen kann.

Es können verschiedene Arten von Host-Namen verwendet werden. In der Regel werden ein frei wählbarer Name und ein Domain-Name verwendet. Bei einem frei wählbaren Namen handelt es sich um einen Aliasnamen für eine IP-Adresse, der von einzelnen Personen zugewiesen und verwendet werden kann. Bei einem Domain-Namen handelt es sich um einen strukturierten Namen in einem hierarchisch organisierten Namespace, der als DNS (Domain Name System) bezeichnet wird. Ein Beispiel für einen Domain-Namen ist www.microsoft.de.

Frei wählbare Namen werden über Einträge in der Datei "Hosts" aufgelöst. Diese Datei befindet sich im Ordner "systemroot\System32\Drivers\etc".

Zum Auflösen von Domain-Namen werden DNS-Namensabfragen an einen konfigurierten DNS-Server gesendet. Beim DNS-Server handelt es sich um einen Rechner, auf dem Einträge mit Zuordnungen von Domain-Namen zu IP-Adressen oder Informationen über andere DNS-Server gespeichert sind. Der DNS-Server löst den abgefragten Domain-Namen in eine IP-Adresse auf und sendet das Ergebnis zurück.

Sie müssen Ihre Rechner mit der IP-Adresse des zuständigen DNS-Servers konfigurieren, um Domain-Namen auflösen zu können. Sie müssen Active Directory-basierte Rechner unter Windows oder Betriebssystemen der Windows Server-Produktfamilie mit der IP-Adresse eines DNS-Servers konfigurieren.

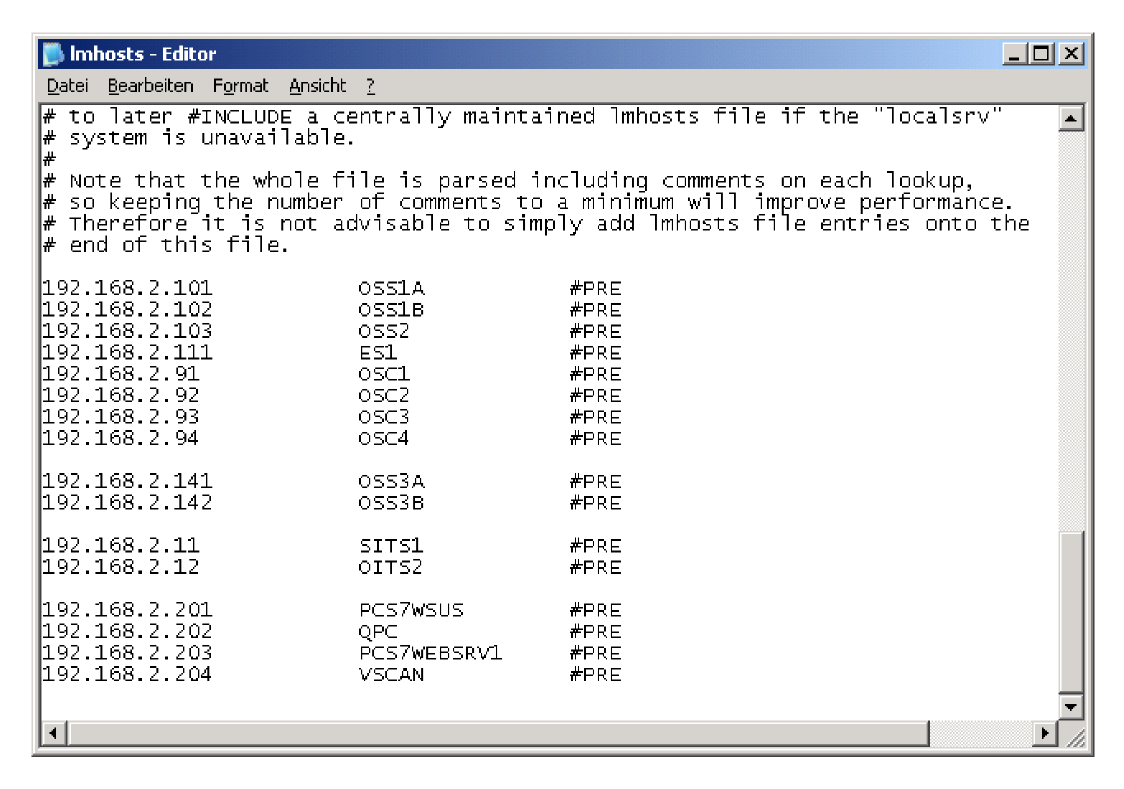
Musterkonfiguration: Namensauflösung

Die Musterkonfiguration wurde in vier bzw. fünf Sicherheitszellen (DCS1, DCS2, MES und Perimeter) aufgeteilt. In keinem dieser Sicherheitszellen ist für die NetBIOS-Namensauflösung ein WINS-Server vorhanden. Ein DNS-Server zur Host-Namensauflösung ist auch in keiner Sicherheitszelle vorhanden. Um eine problemlose Namensauflösung zu gewährleisten, muss auf jedem Rechner die "lmhosts"-Datei konfiguriert werden.

Zuvor muss für jeden Rechner ein Rechnername vergeben werden. Gehen Sie dazu vor, wie unter Punkt "Ändern des Computernamens" beschrieben. Beachten Sie, dass der Rechnername nur vor der Installation von SIMATIC PCS 7 und vor dem ersten Öffnen des WinCC-Explorer geändert werden darf.

Wenn für jeden Rechner ein Rechnername und eine IP-Adresse festgelegt wurden, können Sie die "lmhosts"-Datei konfigurieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Datei "Lmhosts.sam" (z. B. Mithilfe der Anwendung "Notepad".
   Die Datei befindet sich im Verzeichnis "%windir%\system32\Drivers\etc" und ist eine Beispieldatei (Sample), die Sie zur Erstellung der individuellen Lmhosts-Datei als Vorlage verwenden können.
2. Fügen Sie am Ende der Datei für jeden Rechner der Anlage eine neue Zeile ein.



lmhosts - Editor

Datei Bearbeiten Format Ansicht ?

```
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.

192.168.2.101        OSS1A        #PRE
192.168.2.102        OSS1B        #PRE
192.168.2.103        OSS2         #PRE
192.168.2.111        ES1          #PRE
192.168.2.91         OSC1         #PRE
192.168.2.92         OSC2         #PRE
192.168.2.93         OSC3         #PRE
192.168.2.94         OSC4         #PRE

192.168.2.141        OSS3A        #PRE
192.168.2.142        OSS3B        #PRE

192.168.2.11         SITS1        #PRE
192.168.2.12         OITS2        #PRE

192.168.2.201        PCS7WSUS     #PRE
192.168.2.202        QPC          #PRE
192.168.2.203        PCS7WEBSRV1  #PRE
192.168.2.204        VSCAN        #PRE
```

3. Konfigurieren Sie alle Rechner, auch die, die sich in den Sicherheitszellen "MES", "Perimeter", "DCS1" und "DCS2" befinden.
4. Speichern Sie die Datei über den Befehl "Speichern unter" und vergeben Sie der Datei den Namen "Lmhosts" (ohne Dateierweiterung).
5. Kopieren Sie die Datei von dem Rechner, auf dem Sie sie erstellt haben, auf alle Rechner der Anlage.

3.4 Verwaltung von Netzwerken und Netzwerkdiensten

Die Verwaltung der Netzwerkeinstellungen und benötigten Netzwerkdienste eines Prozessleitsystems kann dezentral oder zentral organisiert werden. Mischkonfigurationen von zentraler und dezentraler Verwaltung sind möglich.

Zentrale Verwaltung (Domain, Active Directory)

Alle notwendigen Informationen und Einstellungen können zentral konfiguriert werden:

- IPv4-Adressen, Subnetzmaske, Standard-Gateway, DNS-Server über DHCP
- DNS- und NetBIOS-Namensauflösung über DNS bzw. WINS
- Uhrzeitsynchronisation NTP, SNTP

Dezentrale Verwaltung (Windows-Arbeitsgruppen)

Alle notwendigen Informationen und Einstellungen müssen lokal an jedem einzelnen Rechner innerhalb des Prozessleitsystems konfiguriert werden.

RADIUS

RADIUS (Remote Access Dial In User Service) ist ein Netzwerkprotokoll für die zentrale Authentifikation, Autorisierung und Benutzerkontenführung. Die zentrale Benutzerauthentifizierung von Netzwerkkomponenten ist vorzugsweise über einen zentralen RADIUS-Server durchzuführen, z. B. über den Network Policy Server (NPS) als Teil des MS Active Directory. Informationen zur Konfiguration der RADIUS-Optionen der Netzwerkgeräte finden Sie in den Handbüchern der Scalance X-Netzwerkgeräte.

DHCP

Durch DHCP (Dynamic Host Configuration Protocol) können automatisch Client-Rechner und andere TCP/IP-basierte Netzwerkgeräte mit gültigen IP-Adressen bereitgestellt werden. Es können auch die zusätzlichen, von diesen Clients und Geräten benötigten Konfigurationsparameter, z. B. DNS-Server, WINS-Server, Standard-Gateway, Subnetzmaske bereitgestellt werden.

DHCP wurde im Hinblick auf die zwei folgenden Einsatzszenarien entwickelt:

- Große Netzwerke mit häufig wechselnder Topologie
- Anwender, die "nur eine Netzwerkverbindung" haben möchten und sich nicht näher mit der Netzwerkkonfiguration beschäftigen möchten

Beide Einsatzszenarien treffen auf ein Automatisierungssystem nicht zu. Beim Einsatz von DHCP werden mehrere Sicherheitsrisiken eingegangen, die die Vorteile in einer Automatisierungsanlage nicht ausgleichen können.

Hinweis

Einsatz eines DHCP-Servers

Der Einsatz eines DHCP-Servers zur automatischen Netzwerkkonfiguration (IPv4-Adresse, Subnetzmaske, …) ist aus Sicherheitsgründen nicht empfehlenswert.

Wenn ein DHCP-Server eingesetzt wird, müssen Adressreservierungen verwendet werden.

3.5 Zugangspunkte zu den Sicherheitszellen

3.5.1 Übersicht

Die Sicherheitszellen müssen so gestaltet werden, dass sie u.a. nur einen Zugangspunkt haben. Jeglicher Zugriff auf eine Sicherheitszelle über diesen Zugangspunkt darf nur nach der Überprüfung der Rechtmäßigkeit (bei Personen und Geräten müssen diese authentifiziert und autorisiert werden) erfolgen und muss protokolliert werden. Die Zugangspunkte sollen den unerlaubten Datenverkehr zu den Sicherheitszellen verhindern aber den erlaubten und notwendigen Datenverkehr, der zum reibungslosen Betrieb der Anlage notwendig ist, ermöglichen.
Der Zugangspunkt zu einer Sicherheitszelle kann je nach Erforderlichkeiten bezüglich Konfiguration und Funktionalität unterschiedlich ausgeführt sein.

Informationen zu den unterschiedlichen Konzepten finden Sie im Handbuch "SIMATIC Prozessleitsystem PCS 7 Sicherheitskonzept PCS 7 & WinCC (Basis)" (http://support.automation.siemens.com/WW/view/de/60119725).

3.5.2 Automation Firewall Appliance

Zur Umsetzung bzw. Realisierung der unterschiedlichen Lösungen für Zugangspunkte entsprechend dem Sicherheitskonzept PCS 7 & WinCC (Front/Back Firewall, Threehomed Firewall oder Accesspoint Firewall) steht als SIMATIC PCS 7 Add-on die Automation Firewall Appliance zur Verfügung.

Die momentane Lösung der Automation Firewall basiert auf der Firewall-Lösung von Microsoft (Microsoft Forefront Threat Management Gateway 2010). Mittels des Industrial Wizards und des integrierten SecureGUARD Appliance Managements kann eine optimierte Regelbasis erstellt werden.

Hinweis

Die aktuelle Lösung der Automation Firewall basiert auf dem Microsoft Forefront TMG 2010 . Dieses Produkt von Microsoft ist seit Dezember 2012 nicht mehr verfügbar. Eine alternative Firewall-Lösung wird zurzeit evaluiert. Ein endgültiges Ergebnis lag zur Veröffentlichung des Dokumentes jedoch noch nicht vor.

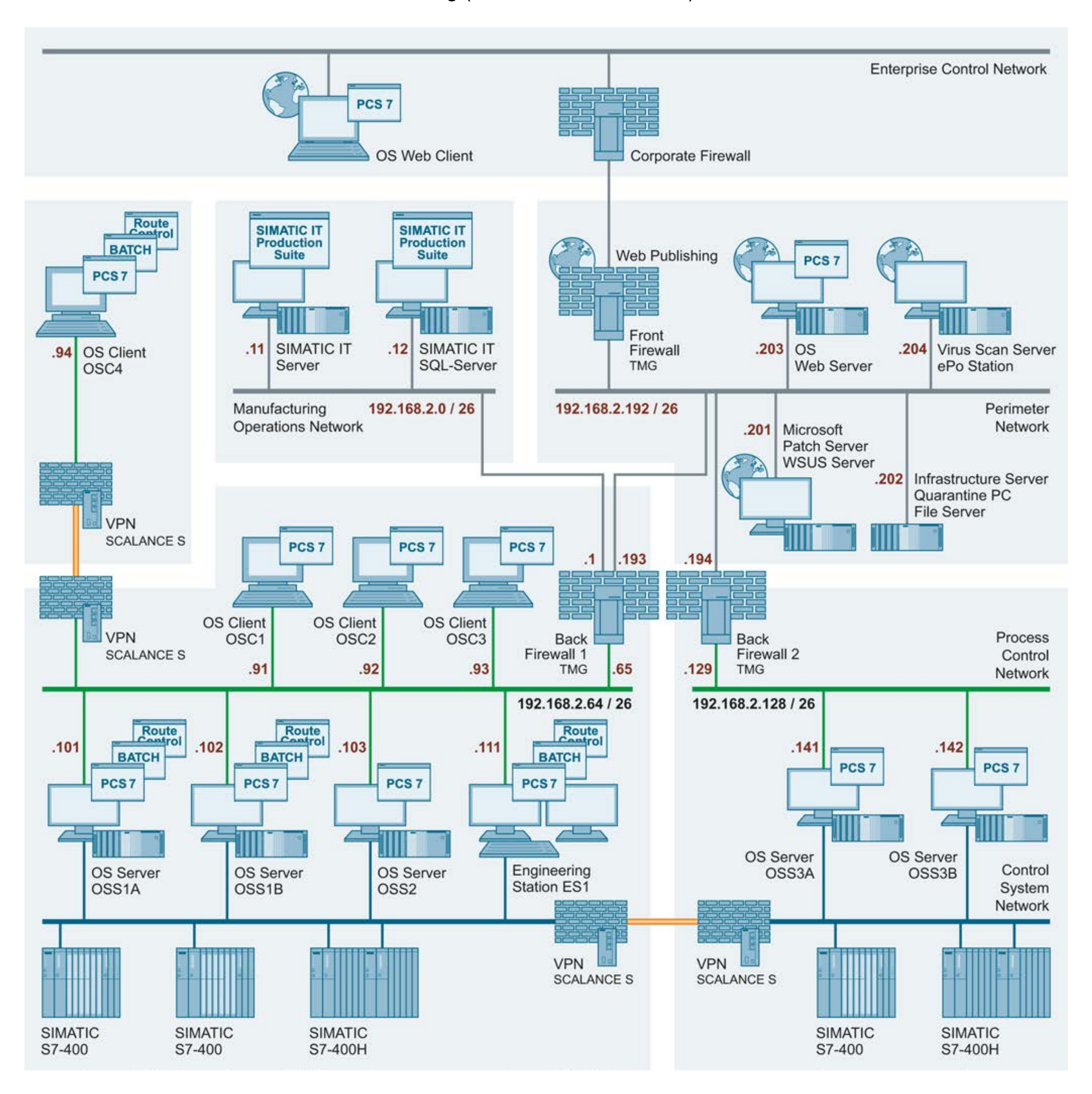
Aus diesem Grund werden im weiteren Verlauf die notwendigen Firewall Regeln neutral formuliert.

Das komplette Angebot zur Automation Firewall finden Sie im PCS 7 Add on-Katalog. Diesen Katalog können Sie über die SIMATIC PCS 7 Webseite (https://www.automation.siemens.com/mcms/process-control-systems/de/simatic-pcs-7/Pages/simatic-pcs-7.aspx) herunterladen.

3.5.3 Musterkonfiguration: Zugriffsregeln

Zugriffsregeln

Bei der Musterkonfiguration werden die Zugangspunkte zu den vier Sicherheitszellen (DCS1, DCS2, MES und Perimeter) durch Firewalls gesichert. Es ergibt sich dabei eine Front/Back Firewall Lösung (mit zwei Back Firewalls).



Um einen uneingeschränkten Betrieb zu gewährleisten, ist ein Datenaustausch zwischen den unterschiedlichen Sicherheitszellen notwendig. Um diesen Datenaustausch zu gewährleisten, müssen in den Firewalls, die als Zugangspunkt zu den Sicherheitszellen fungieren, entsprechende Zugriffsregeln hinterlegt werden.

Der folgenden Tabelle kann der notwendige, sicherheitszellenübergreifende Datenaustausch entnommen werden:

Sicherheitszelle	Sicherheitszelle	Über	Zweck
Perimeter	DSC1	Back Firewall 1	• Verteilung der Windows Updates (Sicherheitsupdates und kritische Updates) mittels PCS7WSUS auf alle Rechner innerhalb des PCN1 • Verteilung der Virensignaturdateien mittels VSCAN auf alle Rechner innerhalb des PCN1 • Kommunikation zw. PCS7WEBSRV1 und OSS1A/B, OSS2 und ES1 • Dateiübertragung zw. QPC und ES1
Perimeter	DCS2	Back Firewall 2	• Verteilung der Windows Updates (Sicherheitsupdates und kritische Updates) mittels PCS7WSUS auf alle Rechner innerhalb des PCN2 • Verteilung der Virensignaturdateien mittels VSCAN auf alle Rechner innerhalb des PCN2 • Kommunikation zwischen PCS7WEBSRV1 und OSS3A/B
Perimeter	MES	Back Firewall 1	• Verteilung der Windows Updates (Sicherheitsupdates und kritische Updates) mittels PCS7WSUS auf alle Rechner innerhalb des MON • Verteilung der Virensignaturdateien mittels VSCAN auf alle Rechner innerhalb des PCN2
MES	DCS1		Kommunikation zwischen den SIMATIC IT Servern und OSS1A/B und OSS2
DCS1	DCS2	Back Firewall 1 und 2	• Kommunikation zwischen OSS3A/B im PCN2 und den OS-Clients im PCN1 • Kommunikation zwischen OSS3A/B im PCN2 und der ES1 im PCN1

Aufgrund der oben abgebildeten Tabelle ergeben sich für die Back Firewall 1 und 2 die folgenden Zugriffsregeln:

- Musterkonfiguration: Zugriffsregeln für die Back Firewall 1

Name	Action	Protocols	From	To
Perimeter WSUS to PCN1 OS-Server #1	Allow	HTTP, HTTPS	[WSUS] [192.168.2.201]	[OS – Server] [192.168.2.101, 192.168.2.102] [OS – Server] [192.168.2.103]
PCN1 OS-Server to Perimeter WSUS #1	Allow	HTTP, HTTPS	[OS – Server] [192.168.2.103]	[WSUS] [192.168.2.201]
PCN1 OS-Server to Perimeter WSUS #2	Allow	HTTP, HTTPS	[OS – Server] [192.168.2.101, 192.168.2.102]	[WSUS] [192.168.2.201]
Perimeter Virenscan-Server to PCN1 OS-Server #1	Allow	HTTP, HTTPS	PatternUpdate] [192.168.2.204]	[OS – Server] [192.168.2.101, 192.168.2.102] [OS – Server] [192.168.2.103]
PCN1 OS-Server to Perimeter Virenscan-Server #1	Allow	HTTP, HTTPS	[OS – Server] [192.168.2.103]	[PatternUpdate] [192.168.2.204]
PCN1 OS-Server to Perimeter Virenscan-Server #2	Allow	HTTP, HTTPS	[OS – Server] [192.168.2.101, 192.168.2.102]	[PatternUpdate] [192.168.2.204]
PCN1 OS-Server to Perimeter OS WebNavigator #1	Allow	IPSec[1]	[OS – Server] [192.168.2.103]	[OS - WebNavigator] [192.168.2.203]
PCN1 OS-Server to Perimeter OS WebNavigator #2	Allow	IPSec[1]	[OS – Server] [192.168.2.101, 192.168.2.102]	[OS - WebNavigator] [192.168.2.203]
Allow Web Servers to access PCN1 #1	Allow	IPSec[1]	[OS - WebNavigator] [192.168.2.203]	[OS – Server] [192.168.2.101, 192.168.2.102] [OS – Server] [192.168.2.103]
1) Die Verwendung des Protokolltyps "IPSec" setzt voraus, dass entsprechend dem Sicherheitskonzept zwischen den Komponenten in den verschiedenen Sicherheitszellen eine zertifikatsbasierte signierte Verbindung mittels IPSec besteht. Besteht eine solche Verbindung nicht, kann auch "All outbund traffic" eingestellt werden. Allerdings verzichtet man bei einer solchen FW-Regel auf die Portfilterung.				

- Musterkonfiguration: Zugriffsregeln für die Back Firewall 2

Name	Action	Protocols	From	To
Perimeter WSUS to PCN2 OS-Server #1	Allow	HTTP, HTTPS	[WSUS] [192.168.2.201]	[OS – Server] [192.168.2.141, 192.168.2.142]
PCN2 OS-Server to Perimeter WSUS #1	Allow	HTTP, HTTPS	[OS – Server] [192.168.2.141, 192.168.2.142]	[WSUS] [192.168.2.201
Perimeter Virenscan-Server to PCN2 OS-Server #1	Allow	HTTP, HTTPS	[PatternUpdate] [192.168.2.204]	[OS – Server] [192.168.2.141, 192.168.2.142]
PCN2 OS-Server to Perimeter Virenscan-Server #1	Allow	HTTP, HTTPS	[OS – Server] [192.168.2.141, 192.168.2.142]	[PatternUpdate] [192.168.2.204]
PCN2 OS-Server to Perimeter OS WebNavigator #1	Allow	IPSec[1]	[OS – Server] [192.168.2.141, 192.168.2.142]	[OS - WebNavigator] [192.168.2.203]
Allow Web Servers to access PCN1 #1	Allow	IPSec[1]	[OS - WebNavigator] [192.168.2.203]	[OS – Server] [192.168.2.141, 192.168.2.142]

[1)] Die Verwendung des Protokolltyps "IPSec" setzt voraus, dass entsprechend dem Sicherheitskonzept zwischen den Komponenten in den verschiedenen Sicherheitszellen eine zertifikatsbasierte signierte Verbindung mittels IPSec besteht. Besteht eine solche Verbindung nicht, kann auch "All outbund traffic" eingestellt werden. Allerdings verzichtet man bei einer solchen FW-Regel auf die Portfilterung.

In der Musterkonfiguration ist nur eine Engineering Station in der Sicherheitszelle DCS1 vorhanden, die auch für die Projektierung der OS-Server OSS3A und OSS3B eingesetzt wird. Um die Projektierungsschritte, im speziellen das OS-Laden, zu gewährleisten, müssen Sie ebenfalls manuell folgende Zugriffsregeln konfigurieren:

Name	Action	Protocols	From	To
PCN2 OS – Server to PCN ES – Engineering Station #1	Allow	IPSec[1]	[OS – Server] [192.168.2.141, 192.168.2.142]	[ES – Engineering Station] [192.168.2.111]
PCN ES – Engineering Station to PCN2 OS – Server #1	Allow	IPSec[1]	[ES – Engineering Station] [192.168.2.111]	[OS – Server] [192.168.2.141, 192.168.2.142]

[1)] Die Verwendung des Protokolltyps "IPSec" setzt voraus, dass entsprechend dem Sicherheitskonzept zwischen den Komponenten in den verschiedenen Sicherheitszellen eine zertifikatsbasierte signierte Verbindung mittels IPSec besteht. Besteht eine solche Verbindung nicht, kann auch "All outbund traffic" eingestellt werden. Allerdings verzichtet man bei einer solchen FW-Regel auf die Portfilterung.

Von den OS-Clients im PCN soll auch das Bedienen und Beobachten der OS-Server OSS3A und OSS3B möglich sein. Um dies zu gewährleisten, müssen Sie folgende Zugriffsregeln konfigurieren:

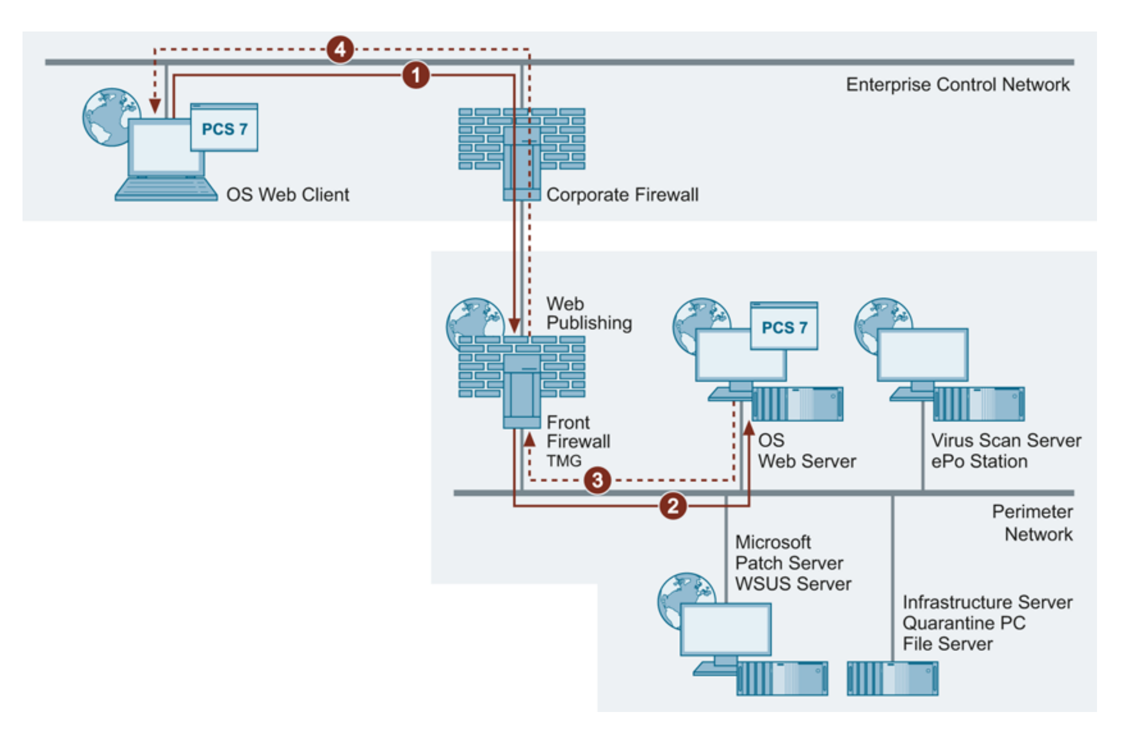
Name	Action	Protocols	From	To
PCN2 OS – Server to PCN OS - Client #1	Allow	IPSec[1]	[OS – Server] [192.168.2.141, 192.168.2.142]	[ES – Client] [192.168.2.91]
PCN2 OS – Server to PCN OS - Client #2	Allow	IPSec[1]	[OS – Server] [192.168.2.141, 192.168.2.142]	[ES – Client] [192.168.2.92]
PCN2 OS – Server to PCN OS - Client #3	Allow	IPSec[1]	[OS – Server] [192.168.2.141, 192.168.2.142]	[ES – Client] [192.168.2.93]
PCN2 OS – Server to PCN OS - Client #4	Allow	IPSec[1]	[OS – Server] [192.168.2.141, 192.168.2.142]	[ES – Client] [192.168.2.94]
PCN OS – Client to PCN2 OS – Server #1	Allow	IPSec[1]	[ES – Client] [192.168.2.91]	[OS – Server] [192.168.2.141, 192.168.2.142]
PCN OS – Client to PCN2 OS – Server #2	Allow	IPSec[1]	[ES – Client] [192.168.2.92]	[OS – Server] [192.168.2.141, 192.168.2.142]
PCN OS – Client to PCN2 OS – Server #3	Allow	IPSec[1]	[ES – Client] [192.168.2.93]	[OS – Server] [192.168.2.141, 192.168.2.142]
PCN OS – Client to PCN2 OS – Server #4	Allow	IPSec[1]	[ES – Client] [192.168.2.94]	[OS – Server] [192.168.2.141, 192.168.2.142]

1) Die Verwendung des Protokolltyps "IPSec" setzt voraus, dass entsprechend dem Sicherheitskonzept zwischen den Komponenten in den verschiedenen Sicherheitszellen eine zertifikatsbasierte signierte Verbindung mittels IPSec besteht. Besteht eine solche Verbindung nicht, kann auch "All outbund traffic" eingestellt werden. Allerdings verzichtet man bei einer solchen FW-Regel auf die Portfilterung.

Musterkonfiguration: Web-Veröffentlichung des PCS 7 Web Server an der Front Firewall

Um auf einen Web Server im Perimeter-Netzwerk aus einem externen Netzwerk zuzugreifen, muss dieser über die Front Firewall veröffentlicht werden. Die Technik der Web-Veröffentlichung, welche von der Automation Firewall unterstützt wird und hierbei zum Einsatz kommt, bietet eine bessere Sicherheit als die veraltete Technik des Web-Tunneling oder Web-Forwarding. Das Öffnen der Ports 80 oder 443 und somit ein einfaches Durchreichen der Anfragen durch die Front Firewall direkt zum Web Server, wie es diese Technik vorsieht, soll nicht mehr angewendet werden.

Bei der Web-Veröffentlichung (siehe nachfolgende Abbildung) greift der Web Client aus dem externen Netzwerk nicht direkt auf den Web Server zu, sondern stellt seine Anfrage an die Automation Firewall (1). Die Automation Firewall reicht die überprüfte Anfrage an den Web Server weiter (2) und bekommt daraufhin die gewünschten Informationen zurück (3). Diese leitet sie anschließend an den Web Client weiter (4).



Zwischen dem Web Client und der Automation Firewall soll nur HTTPS erlaubt werden. So kann die Authentizität des TMG per Server-Zertifikat garantiert und die Kommunikation zwischen Web Client und Firewall verschlüsselt und somit gegen Manipulation geschützt werden. Für den Zugriff der Automation Firewall auf den Web Server kann je nach gewünschter interner Sicherheit entweder HTTP oder HTTPS verwendet werden.

Sollen Web Clients aus einem externen Netz auf den Web Server zugreifen, muss dieser an der Front Firewall veröffentlicht werden. Sollen hingegen Web Clients aus einem MES-Netz (MON) zugreifen können, erfolgt die Veröffentlichung an der Back Firewall.

Hinweis

Die Schritte zur Projektierung des OS Web Servers sowie die Einstellungen des Web Clients entnehmen Sie dem Handbuch "SIMATIC Prozessleitsystem PCS 7 V7.0 PCS 7 OS Web Option" (http://support.automation.siemens.com/WW/view/de/24496095).

Musterkonfiguration: Web-Veröffentlichung des PCS 7 Web Server an der Back Firewall

Um den PCS 7 Web Server, der sich im Perimeter-Netzwerk befindet, von einem anderen internen Netzwerk z. B. vom Manufacturing Operations-Netzwerk (MON) per Web Client zu erreichen, muss der Web Server an der Back Firewall 1 veröffentlicht werden.
Da diese Funktionalität im Industrial Wizard nicht implementiert ist, müssen Sie in diesem Fall die Veröffentlichungsregel mittels der Microsoft Forefront TMG Management Konsole in der Back Firewall erstellen.

Network Intrusion Prevention / Network Intrusion Detection System

Ein Intrusion Detection bzw. Intrusion Prevention System (IDS/IPS) ist ein wesentlicher Bestandteil eines modernen, sicheren Web-Gateways. Das Network Inspection System (NIS) in Microsoft Forefront TMG 2010 ist eine Umsetzung der IDS/IPS Funktionalität. NIS ist speziell auf die Erkennung und Unterbindung von Angriffen auf Microsoft-Betriebssystemen und Anwendungen konzipiert. NIS basiert auf Signaturen, die durch das Microsoft Malware Protection Center (MMPC) entwickelt und über Windows Update oder WSUS verteilt werden.

NIS in Microsoft Forefront TMG 2010 bietet diesen Schutz vor bekannten Angriffen durch die Low Level-Netzwerkprotokoll Inspektion. Jedes Datenpaket wird auf Protokollstatus, Struktur und Inhalt der Nachricht analysiert. Das NIS überprüft das empfangene Datenpaket erst, nachdem es durch die Firewall Policy und evtl. zugeordnete Web- bzw. Anwendungsfilter überprüft wurde.

Weitere Informationen

Das komplette Angebot zur Automation Firewall finden Sie im PCS 7 Add on-Katalog. Diesen Katalog können Sie über die SIMATIC PCS 7 Webseite (https://www.automation.siemens.com/mcms/process-control-systems/de/simatic-pcs-7/Pages/simatic-pcs-7.aspx) herunterladen.

3.6 Sichere Kommunikation zwischen Sicherheitszellen

3.6.1 Übersicht

In vielen Fällen ist ein Datenaustausch zwischen Komponenten, die sich in unterschiedlichen Sicherheitszellen befinden, für den normalen Betrieb einer Anlage notwendig. Dabei sind folgende Varianten zu unterscheiden:

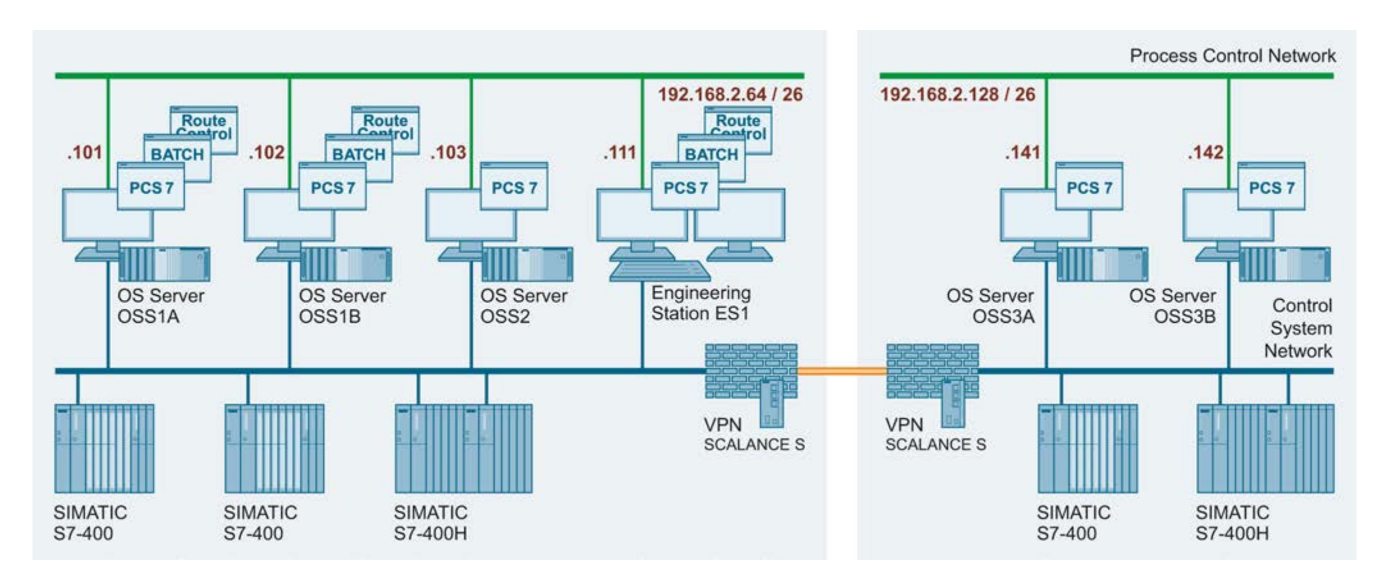
- Datenaustausch auf CSN-Ebene
  Datenaustausch zwischen Automatisierungssystemen in unterschiedlichen Sicherheitszellen
- Datenaustausch auf PCN-Ebene
  Datenaustausch zur Bedienung und Beobachtung mit abgesetzten OS-Clients (d.h. OS-Clients, die sich in anderen Sicherheitszellen befinden wie der/die zugehörige(n) OS-Server)

3.6.2 Datenaustausch zwischen Automatisierungssystemen

3.6.2.1 Einführung

Der Datenaustausch zwischen Automatisierungssystemen in unterschiedlichen Sicherheitszellen soll mittels VPN-Verbindung (IPSec) erfolgen. Diese Kommunikation kann mittels zweier SCALANCE S-Sicherheitsmodule aufgebaut werden.

Die folgende Abbildung zeigt beispielsweise die Kommunikation zwischen Automatisierungssystemen unterschiedlicher Sicherheitszellen:



In den von SCALANCE S geschützten internen Netzen stellen IPSec-Tunnel den Knoten für eine gesicherte Datenverbindung durch das unsichere externe Netz zur Verfügung.

Der Datenaustausch der Geräte über die IPSec-Tunnel im VPN hat dadurch folgende Eigenschaften:

- Die ausgetauschten Daten sind abhörsicher und somit ist die Vertraulichkeit der Daten gesichert.
- Die ausgetauschten Daten sind verfälschungssicher, somit ist die Integrität der Daten gesichert.
- Authentizität

SCALANCE S verwendet für das Tunneling das IPSec-Protokoll (Tunnelmodus von IPSec).

Hinweis

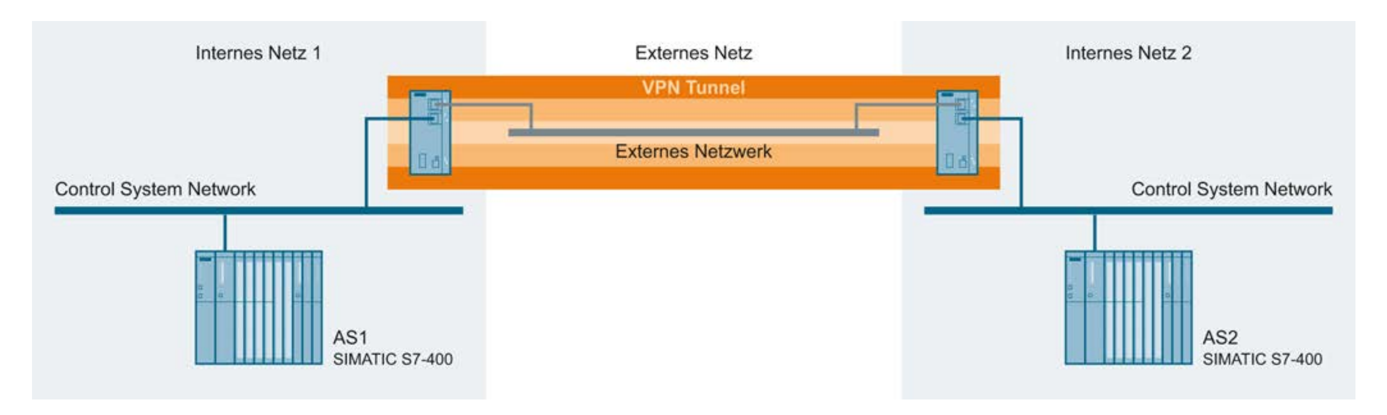
Weitere Informationen zu SCALANCE S finden Sie im Handbuch "SCALANCE S und SOFTNET Security Client" (http://support.automation.siemens.com/WW/view/de/21718449).

3.6.2.2 Musterkonfiguration: Aufbau einer sicheren Kommunikation zwischen Sicherheitszellen mit SCALANCE S

Einleitung

In diesem Beispiel wird die Tunnelfunktion in der Projektierungssicht "Standard-Modus" projektiert. SCALANCE S Modul 1 und SCALANCE S Modul 2 bilden in diesem Beispiel die beiden Tunnelendpunkte für die gesicherte Tunnelverbindung.

Die folgende Abbildung zeigt beispielsweise einen VPN-Tunnel (IPSec-Tunnel mit zwei SCALANCE S Modulen):



Das interne (sichere) Netzwerk wird am SCALANCE S am Port 2 ("Internal Network"-Port) angeschlossen. Im internen Netzwerk wird der Netzknoten jeweils durch ein Automatisierungssystem repräsentiert, das an den "Internal Network"-Port 2 (Port2 = grün) eines SCALANCE S Moduls angeschlossen ist.

- AS1: Repräsentiert einen Teilnehmer des CSN in der Sicherheitszelle 1 (internes Netz 1)
- AS2: Repräsentiert einen Teilnehmer des CSN in der Sicherheitszelle 2 (internes Netz 2)
- SCALANCE S Modul 1: SCALANCE S Modul für die Sicherheitszelle 1
- SCALANCE S Modul 2: SCALANCE S Modul für die Sicherheitszelle 2

Das öffentliche, externe Netzwerk ("unsicheres Netz") wird an den "External Network"-Port (Port1 = rot) des SCALANCE S Moduls angeschlossen.

Projektierungsschritte im Überblick

1. SCALANCE S und Netzwerke einrichten
2. IP-Einstellungen der Automatisierungssysteme einrichten
3. Projekt und Modul anlegen
4. Tunnel-Funktion projektieren
5. Konfiguration in SCALANCE S laden
6. Test

SCALANCE S und Netzwerke einrichten

Um SCALANCE S und die Netzwerkverbindungen einzurichten, gehen Sie folgendermaßen vor:

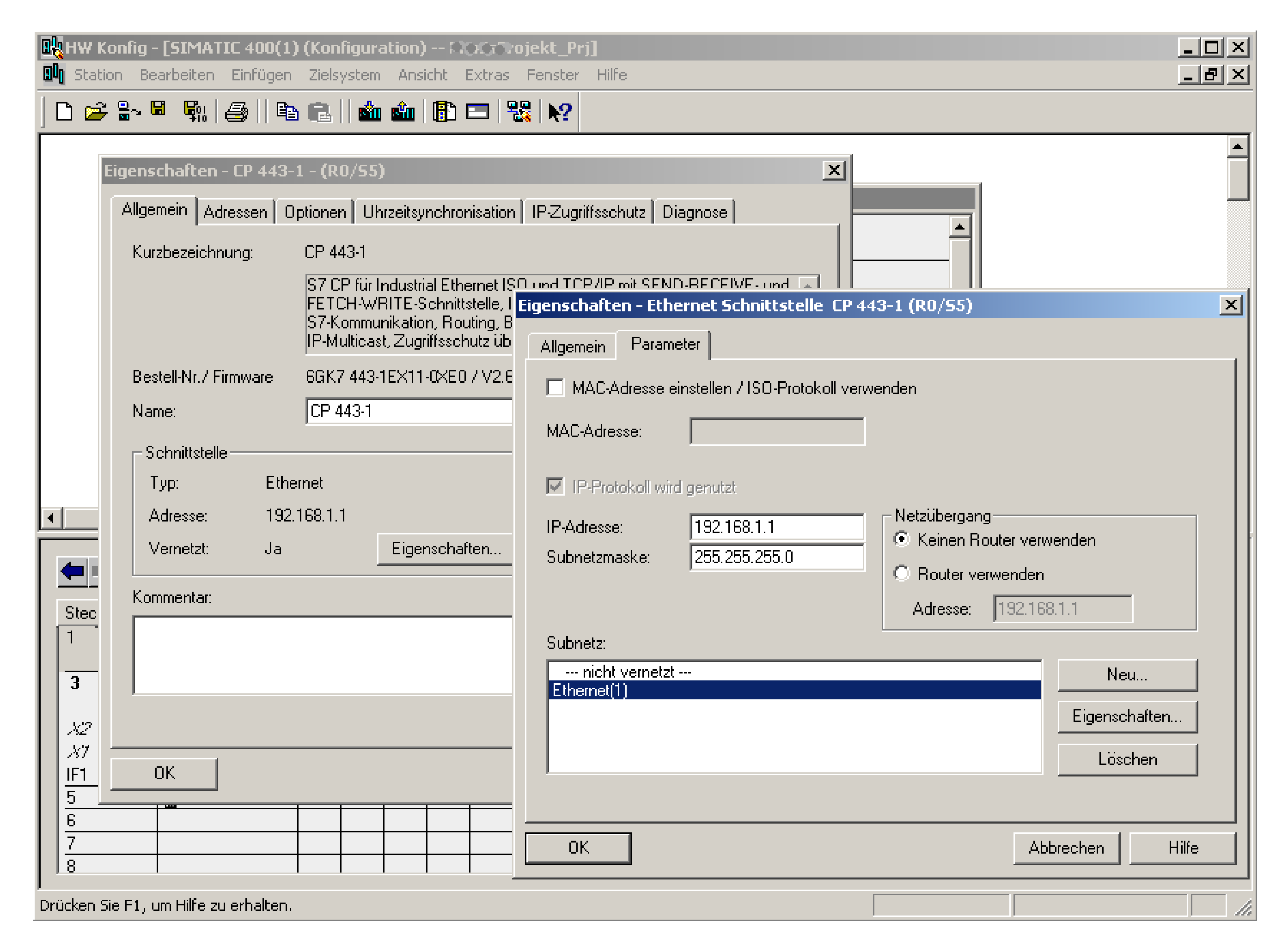
1. Nehmen Sie den SCALANCE S entsprechend der Betriebsanleitung in Betrieb.
2. Stellen Sie die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die Ports (RJ45-Buchsen) stecken:
   – Verbinden Sie das Control System-Netzwerk 1 mit Port 2 von Modul 1 und das Control System-Netzwerk 2 mit Port 2 von Modul 2
   – Verbinden Sie Port 1 von Modul 1 und Port 1 von Modul 2 mit einem Netzwerk-Switch und bauen Sie somit das "externe" Netzwerk auf.
   – Schalten Sie die beteiligten Komponenten ein.

IP-Einstellungen der Automatisierungssysteme einrichten

Stellen Sie für die Automatisierungssysteme folgende IPv4-Adresseinstellungen ein:

Automatisierungssystem	IPv4-Adresse	SubNet-Maske
AS 1	192.168.1.1	255.255.255.0
AS 2	192.168.2.1	255.255.255.0

Die folgende Abbildung zeigt beispielhaft, wie die IPv4-Adresse des Automatisierungssystems eingestellt wird:



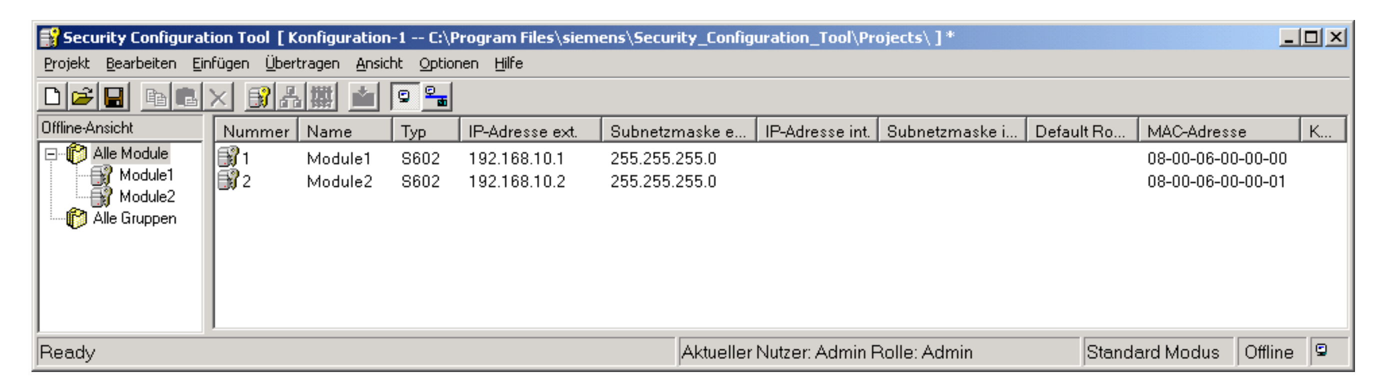
Projekt und Module anlegen

Die Module SCALANCE S612 und S613 werden mit dem Projektierungswerkzeug "Security Configuration Tool" konfiguriert.

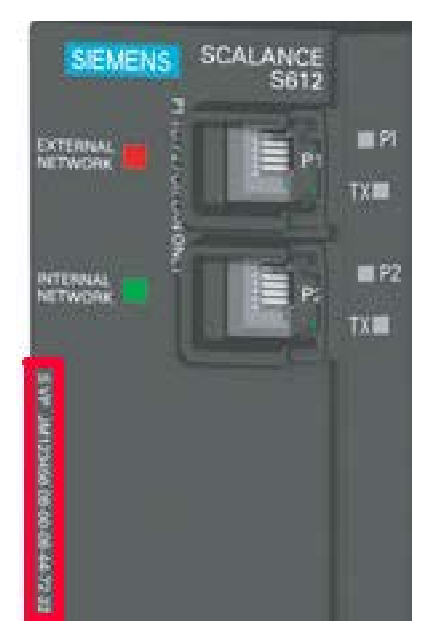
Um das Projekt und die Module für die Musterkonfiguration anzulegen, gehen Sie folgendermaßen vor:

1. Starten Sie die Projektierungssoftware "Security Configuration Tool".
2. Erstellen Sie ein neues Projekt über den Befehl "Projekt > Neu".
   Sie werden aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie festlegen, wird die Rolle eines Administrators zugewiesen.
3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe.
   Ein neues Projekt wird angelegt.
4. Klicken Sie auf "Alle Module".

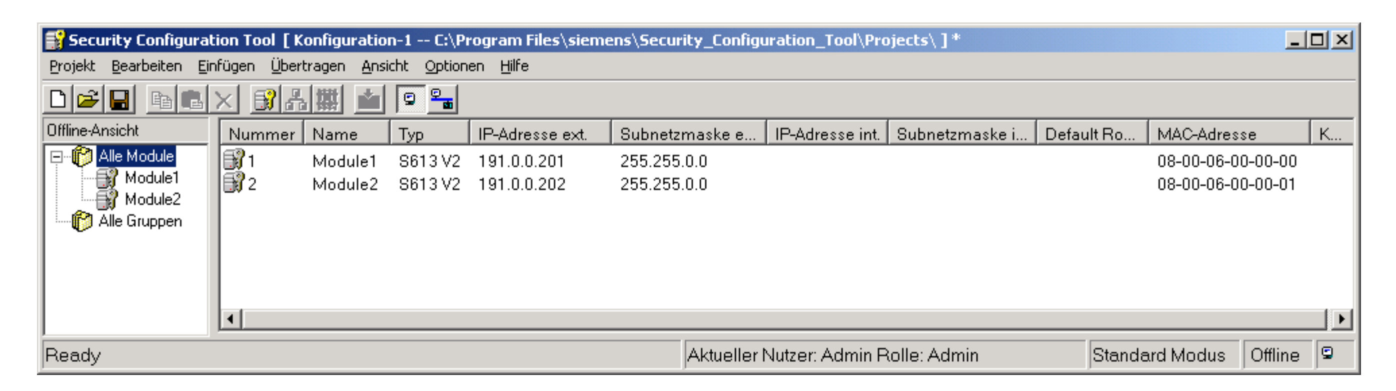
5. Erstellen Sie ein zweites Modul über den Befehl "Einfügen > Modul".
   Das Modul wird eingefügt und erhält automatisch einen Namen entsprechend den Voreinstellungen für das Projekt und voreingestellte Parameterwerte. Die IPv4-Adresse wird gegenüber "Module1" weitergezählt und ist unterschiedlich.



6. Selektieren Sie den Eintrag "Module1".
7. Wählen Sie in der Spalte "Typ" den Typ des verwendeten Moduls aus.
8. Geben Sie in der Spalte "MAC-Adresse" die MAC-Adresse des Moduls im vorgebebenen Format ein.
   Die MAC-Adresse finden Sie auf der Vorderseite des SCALANCE S-Moduls.



9. Geben Sie in der Spalte "IP Adresse ext" die IPv4-Adresse des Moduls im vorgebebenen Format ein und passen Sie die Subnetzmaske an:
   - Für Modul 1: IPv4-Adresse: 191.0.0.201 Subnetzmaske: 255.255.0.0
   - Für Modul 2: IPv4-Adresse: 191.0.0.202 Subnetzmaske: 255.255.0.0



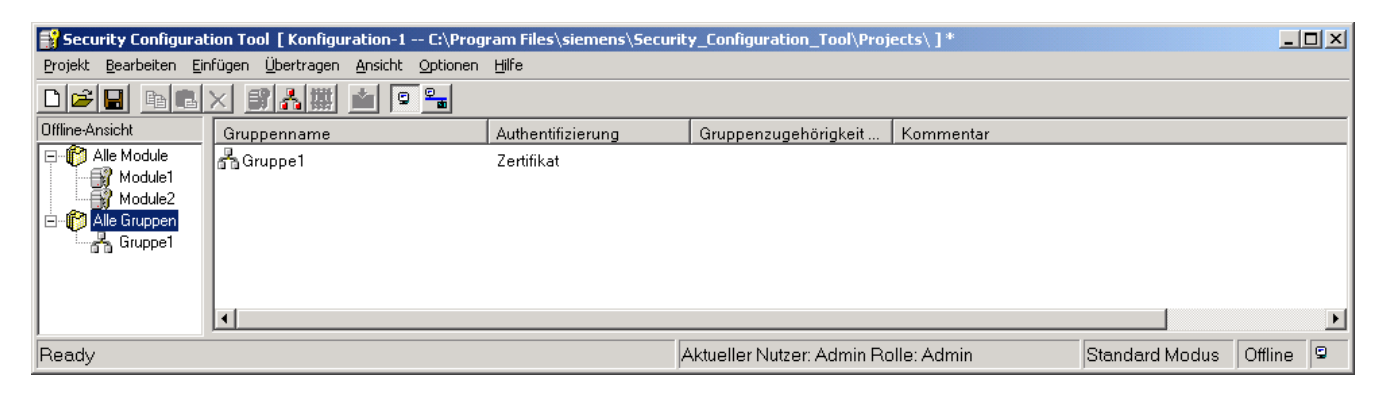
10. Wiederholen Sie die Schritte 6 bis 9 für das Modul "Module2".

Tunnelverbindung projektieren

Zwei SCALANCE S können genau dann einen IPSec-Tunnel für die gesicherte Kommunikation aufbauen, wenn sie im Projekt der gleichen Gruppe zugeordnet sind.

Um eine Tunnelverbindung zu projektieren, gehen Sie folgendermaßen vor:

1. Selektieren Sie im Projektierungswerkzeug "Security Configuration Tool" den Navigationsbereich "Alle Gruppen".
2. Erstellen Sie eine neue Gruppe über den Befehl "Einfügen > Gruppe".
   Die Gruppe wird eingefügt und erhält automatisch den Namen "Gruppe1".



3. Selektieren Sie im Inhaltsbereich das SCALANCE S-Modul "Module1" und ziehen Sie es auf "Gruppe1" im Navigationsbereich.
   Das Modul wird der Gruppe "Gruppe1" zugeordnet. Die Farbe des Schlüsselsymbols des Modul-Icons wird von grau in blau geändert.

4. Selektieren Sie im Inhaltsbereich das SCALANCE S-Modul "Module 2" und ziehen es auf "Gruppe1" im Navigationsbereich.
   Das Modul (Module2) wird ebenso der Gruppe "Gruppe1" zugeordnet.
5. Speichern Sie das Projekt über den Befehl "Projekt > Speichern unter ..." unter einem geeigneten Namen ab.
   Die Konfiguration der Tunnelverbindung ist damit abgeschlossen.

Konfiguration in SCALANCE S laden

Um die erstellte Konfiguration in die SCALANCE S-Module zu laden, gehen Sie folgendermaßen vor:

1. Wählen Sie im Menü "Übertragen" den Befehl "An alle Module ..".

Hinweis

Weitere Informationen über Konfigurationen und Einsatzmöglichkeiten der SIMATIC Security-Produkte finden Sie unter http://support.automation.siemens.com/WW/view/de/67329379 oder im Siemens Industry Online Support Portal.

3.6.3 Quarantäne-Station (File-Server)

Einleitung

Eine Quarantäne-Station ist ein zentraler Datenaustauschpunkt in einer Anlage. Die Quarantäne-Station dient dazu, Daten (z. B. Projektierungs- oder Engineering-Daten) auf bestimmte Rechner innerhalb des Automatisierungssystems bzw. von Rechnern des Automatisierungssystems auf die Quarantäne-Station zu transferieren.

Die Quarantäne-Station ist dann wichtig, wenn die Empfehlungen bezüglich der Systemhärtung im Speziellen dem Sperren der USB-Ports im Automatisierungssystem umgesetzt werden (siehe Kapitel "Umgang mit mobilen Datenträgern (Seite 80)"). Die Quarantäne-Station als zentraler Datenaustauschpunkt ist, aus Security-Sicht, besonders schützenswert. Daher sollen lokale Sicherheitsmaßnahmen (z. B. Firewall, Virenscanner, usw.) ggf. strikter konfiguriert werden.

Die Quarantäne-Station soll, wie bei der Musterkonfiguration dargestellt, im Perimeter-Netzwerk positioniert werden. Um eine Kommunikation zwischen der Quarantäne-Station und den Rechnern in den Sicherheitszellen DCS1 und DCS2 über die Back Firewall(s) zu gewährleisten, müssen in der/den Back Firewall(s) entsprechende Regeln hinterlegt werden.

Firewall-Regeln

Wenn als Back Firewall die Automation Firewall zum Einsatz kommt, kann die Quarantäne-Station (FTP Server) an der Back Firewall für die Sicherheitszellen DCS1 und DCS2 veröffentlicht werden (vgl. Web-Veröffentlichung des PCS 7 Web Server an der Front Firewall oder Web-Veröffentlichung des PCS 7 Web Server an der Back Firewall). Dazu muss eine entsprechende Veröffentlichungsregel (FTP Forwarding) mit dem Task "Publish Non-Web Server Protocols" in der Automation Firewall (Microsoft Forefront TMG Management Konsole) konfiguriert werden:

Name	Action	Traffic	Form	To	Networks
Publish FTP Server	Allow	FTP Server	Anywhere	IP-Adresse der Quarantäne-Station	PCN1

Durch diese FTP-Veröffentlichung des FTP-Servers (Quarantäne-Station) wird, im Vergleich zu einer reinen Port-Freigabe, eine höhere Sicherheit erreicht.

Hinweis

Das komplette Angebot zur Automation Firewall finden Sie im PCS 7 Add on-Katalog. Diesen Katalog können Sie über die SIMATIC PCS 7 Webseite (https://www.automation.siemens.com/mcms/process-control-systems/de/simatic-pcs-7/Pages/simatic-pcs-7.aspx) herunterladen.

Für den Fall, dass eine Firewall zum Einsatz kommt, die die Möglichkeit der FTP-Veröffentlichung nicht bietet, zeigen die folgenden Tabellen die notwendigen Firewall Regeln auf:

- Front Firewall

Name	Action	Protocols	From	To
ECN Computer to Perimeter Q-PC	Allow	FTP / 21	IP-Adresse des Rechners im Office-Netzwerk	IP-Adresse des Q-PC im Perimeter-Netzwerk
Perimeter Q-PC to ECN Computer	Allow	FTP / 21	IP-Adresse des Q-PC im Perimeter-Netzwerk	IP-Adresse des Rechners im Office-Netzwerk

Die Regeln in der Front Firewall sind nur notwendig, wenn ein FTP-Datenzugriff vom ECN (Enterprise Control Network) auf die Quarantäne-Station im Perimeter-Netzwerk möglich ist.

- Back Firewall

Name	Action	Protocols	From	To
Perimeter Q-PC to PCN ... #1	Allow	FTP / 21	IP-Adresse des Q-PC im Perimeter-Netzwerk	IP-Adresse des Rechners im PCNx (z. B. ES1)
PCN … to Perimeter Q-PC #1	Allow	FTP / 21	IP-Adresse des Rechners im PCNx (z. B. ES1)	IP-Adresse des Q-PC im Perimeter-Netzwerk

FTP-Server Konfiguration

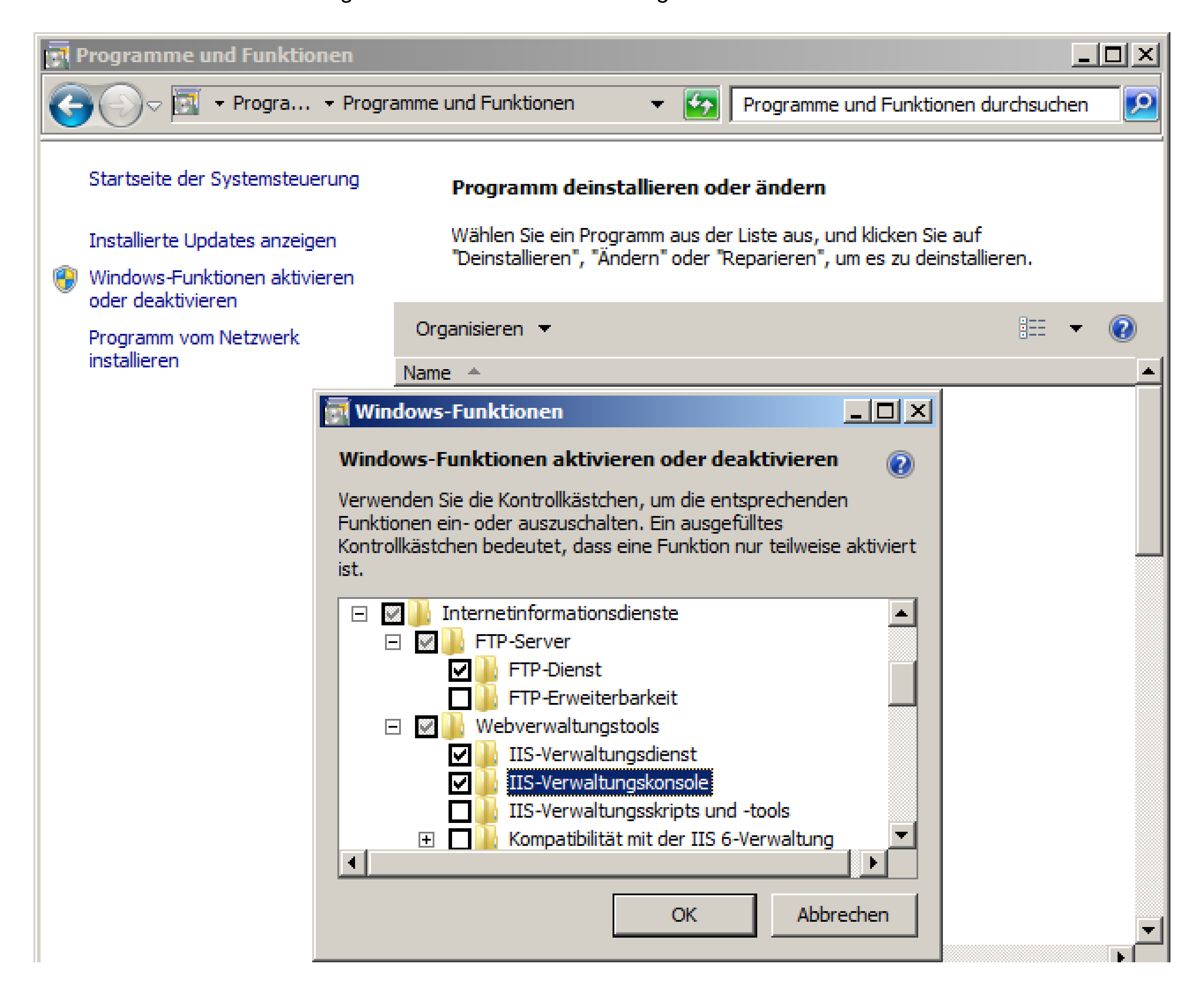
FTP-Dienst aktivieren

Die folgende Vorgehensweise wird am Beispiel des Betriebssystems "Windows 7" beschrieben.

Um auf der Quarantäne-Station den FTP-Dienst zu aktivieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Windows-Startmenü den Befehl "Start > Systemsteuerung > Programme > Programme und Funktionen".
   Der Dialog "Programme deinstallieren oder ändern" wird geöffnet.
2. Klicken Sie im Navigationsbereich auf den Eintrag "Windows-Funktionen aktivieren oder deaktivieren".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie bereits als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung. Der Dialog "Windows-Funktionen" wird geöffnet.
3. Aktivieren Sie im Bereich "Internetinformationsdienste > FTP-Server" die Funktion "FTP-Dienst".

4. Aktivieren Sie im Bereich "Webverwaltungstools" die Funktionen "IIS-Verwaltungskonsole" und "IIS-Verwaltungsdienst".



5. Klicken Sie auf die Schaltfläche "OK", um die Änderungen zu bestätigen.
   Die gewählten Funktionen werden aktiviert.

FTP-Dienst starten

Um den Microsoft FTP-Dienst zu starten, gehen Sie folgendermaßen vor:

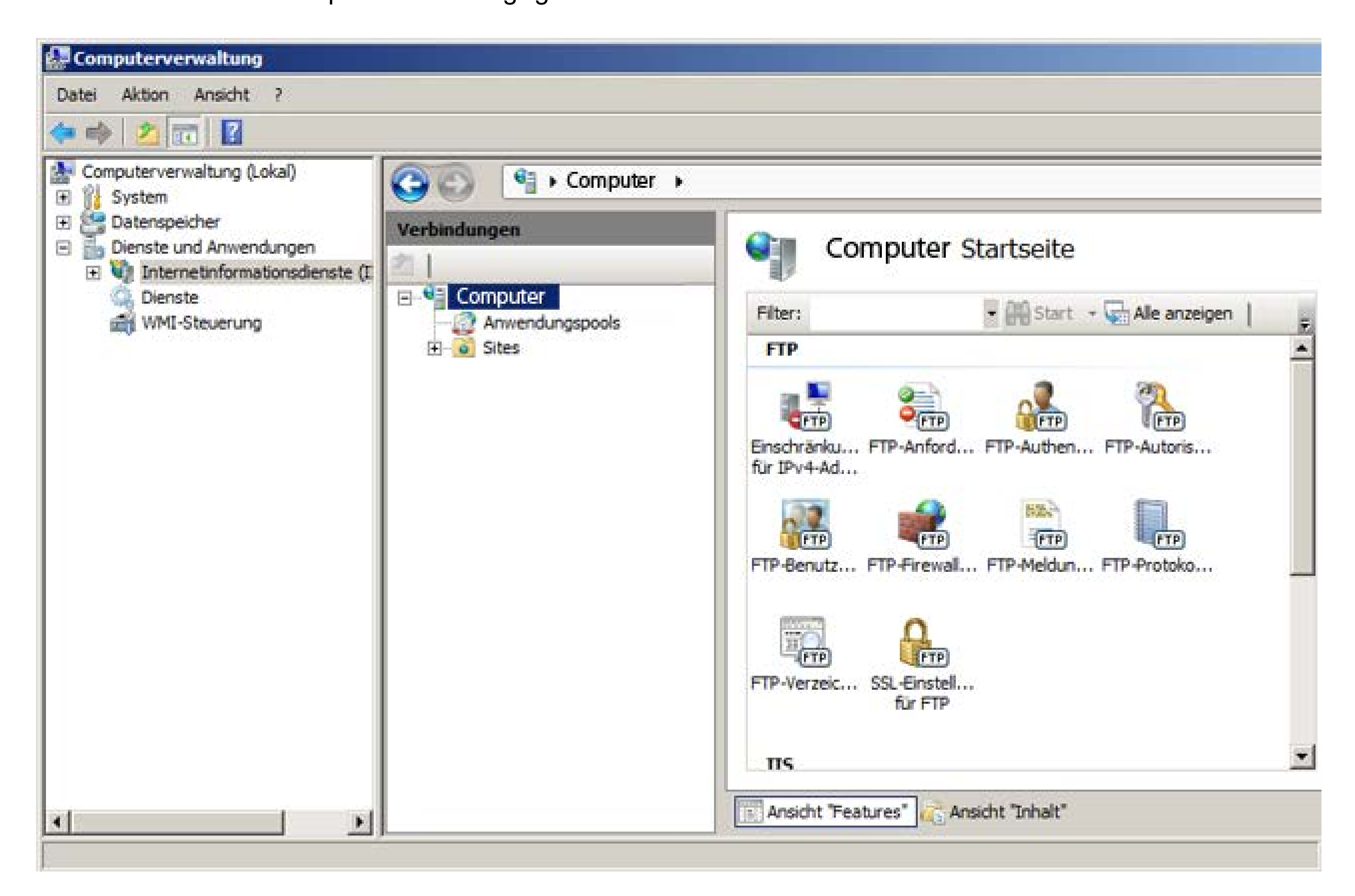
1. Klicken Sie mit der rechten Maustaste auf "Computer" und wählen Sie im Kontextmenü den Befehl "Verwalten".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie bereits als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung. Der Dialog "Computerverwaltung" wird geöffnet.
2. Wählen Sie im Navigationsbereich den Eintrag "Dienste und Anwendungen > Dienste". Im rechten Bereich des Dialogs werden alle verfügbaren Dienste angezeigt.
3. Selektieren Sie den Dienst "Microsoft-FTP-Dienst" und überprüfen Sie die folgenden Eigenschaften:
   - Starttyp: Automatisch
   - Status: Gestartet

   Falls die Eigenschaftswerte abweichen, öffnen Sie den Dialog "Eigenschaften" über das Kontextmenüs des Dienstes und ändern Sie die Eigenschaften wie oben aufgeführt.

FTP-Server konfigurieren

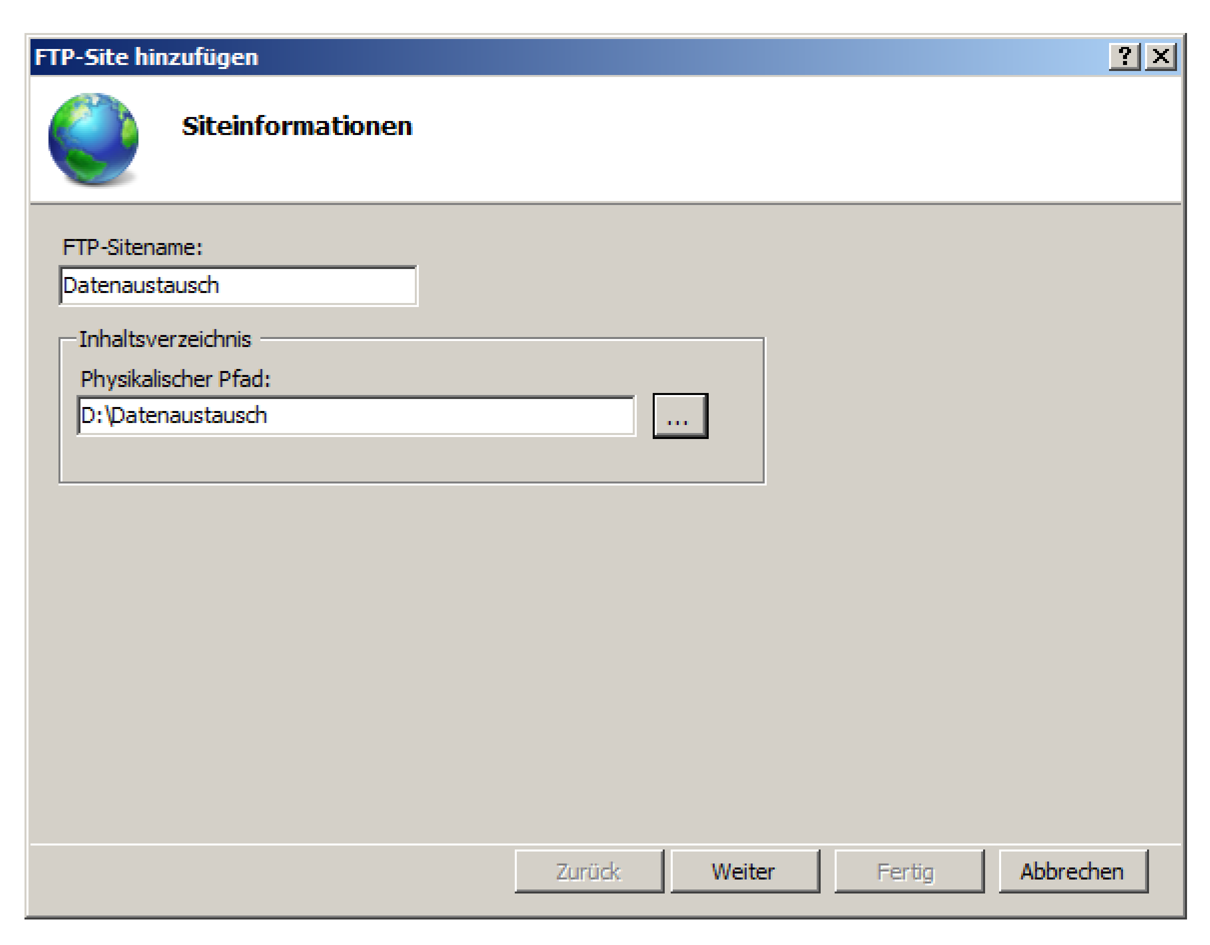
Um den FTP-Server zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Windows Start-Menü mit der rechten Maustaste auf "Computer" und wählen Sie im Kontextmenü den Befehl "Verwalten".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie bereits als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Dialog "Computerverwaltung" wird geöffnet.
2. Klicken Sie im Navigationsbereich auf den Eintrag "Dienste und Anwendungen > Internetinformationsdienste (IIS) Manager".
   Der Internetinformationsdienste (IIS) Manager wird im rechten Bereich des Dialogs "Computerverwaltung" geöffnet.



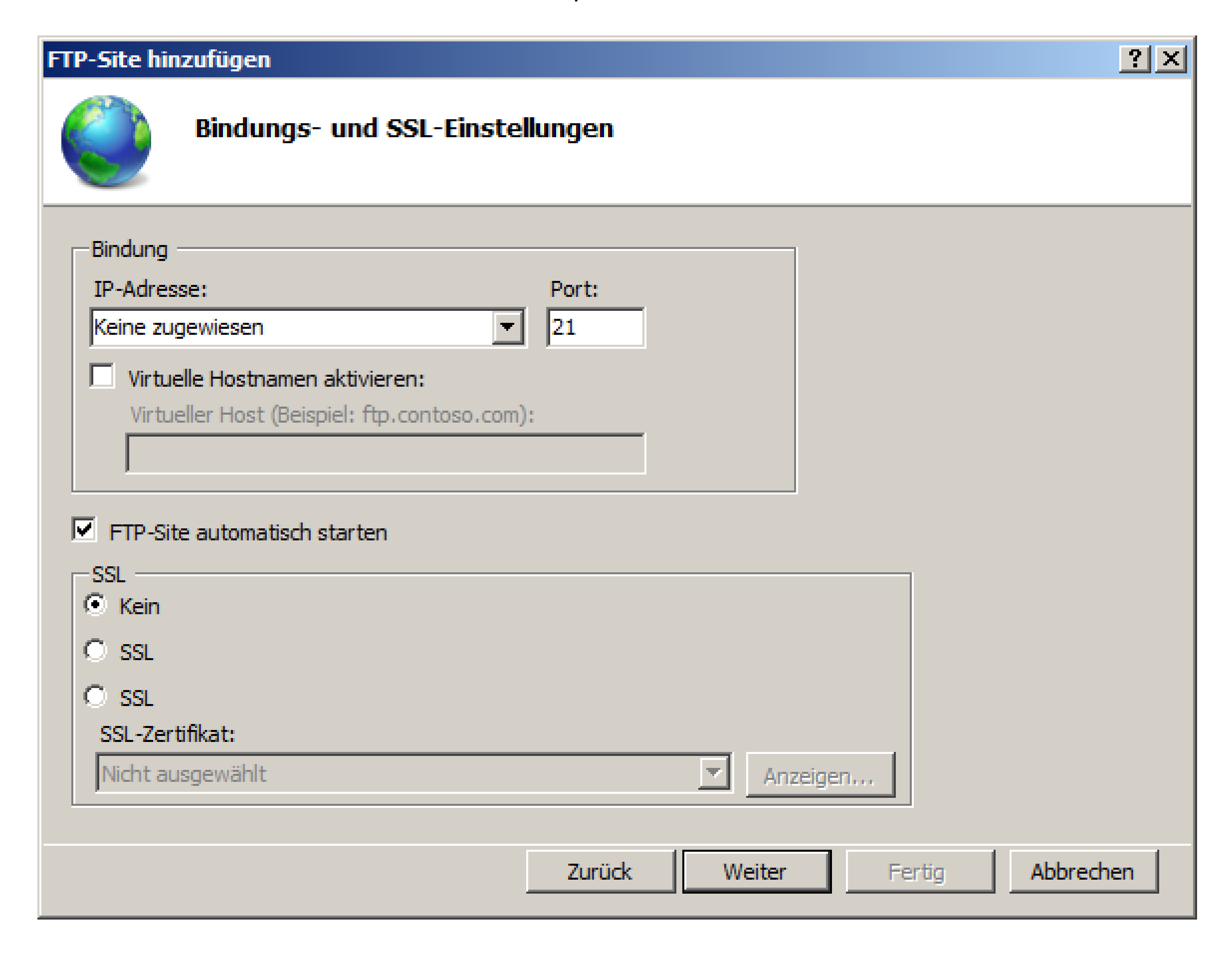
3. Um eine FTP-Site als FTP-Rootverzeichnis einzufügen, legen Sie auf der Daten-Partition (D:\) einen neuen Ordner mit dem Namen "Datenaustausch" (D:\Datenaustausch) an.
4. Klicken Sie mit der rechten Maustaste auf das Symbol „Sites“. Wählen Sie im Kontextmenü den Befehl "FTP-Site hinzufügen…".
   Der Dialog "FTP-Site hinzufügen" wird geöffnet.

5. Geben Sie im Dialog "FTP-Site hinzufügen" einen Namen für die FTP-Site und den physikalischen Pfad zum erstellten Verzeichnis (D:\Datenaustausch) ein.



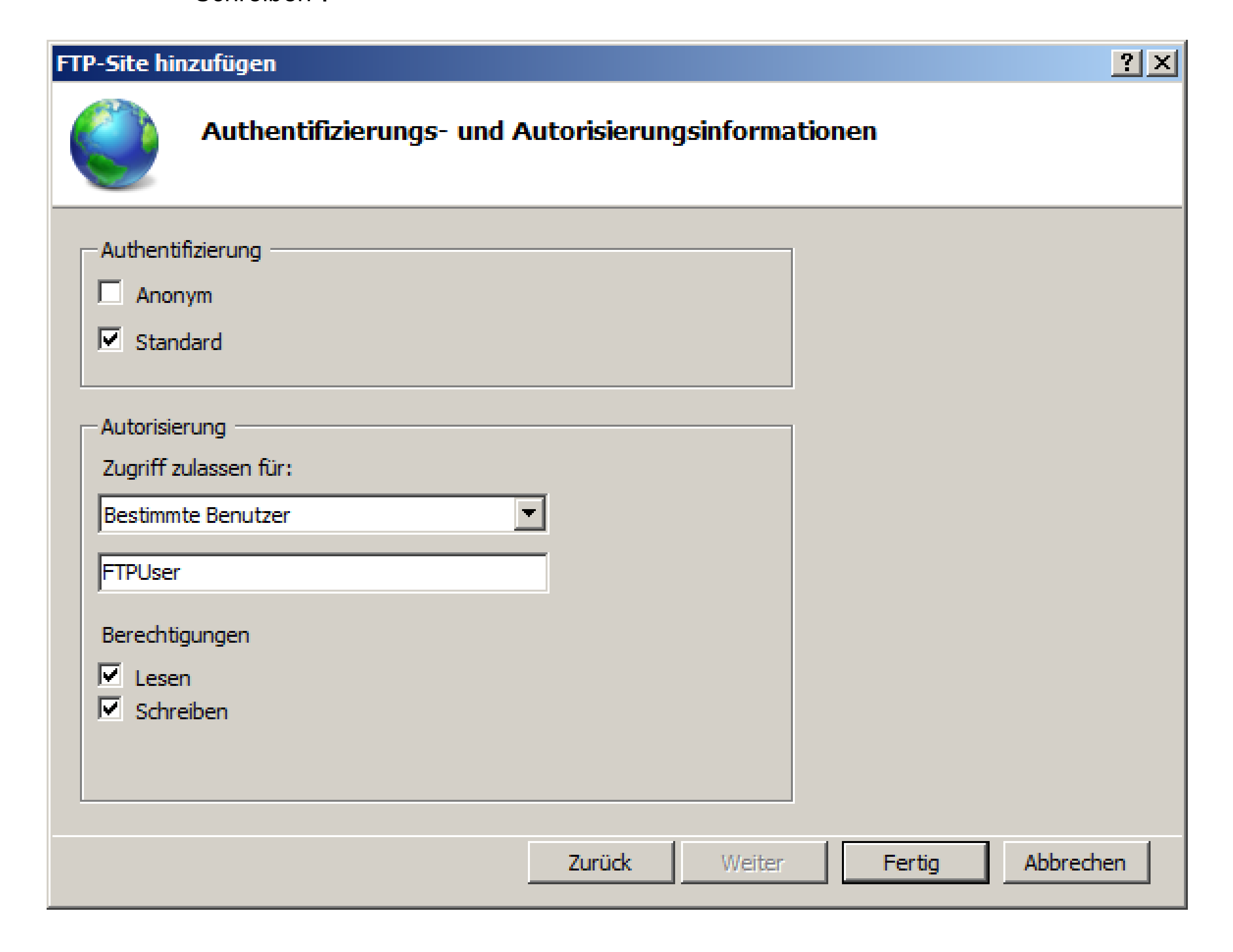
6. Klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog "Bindungs- und SSL-Einstellungen" wird geöffnet.

7. Nehmen Sie im Dialog "Bindungs- und SSL-Einstellungen" die folgenden Einstellungen vor:
   - Bereich "Bindung", Feld "IP-Adresse": Wählen Sie den Eintrag "Keine zugewiesen" aus der Klappliste aus.
   - Bereich SSL: Aktivieren Sie die Option "Kein".



8. Klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog "Authentifizierungs- und Autorisierungsinformationen" wird geöffnet.

9. Nehmen Sie im Dialog "Authentifizierungs- und Autorisierungsinformationen" die folgenden Einstellungen vor:
   - Bereich "Autorisierung > Zugriff zugelassen für": Wählen Sie den Eintrag "Bestimmte Benutzer" aus der Klappliste und geben Sie die zugelassenen Benutzer in das Feld darunter ein.
   - Bereich "Berechtigungen": Aktivieren Sie die Kontrollkästchen "Lesen" und "Schreiben".



10. Klicken Sie auf die Schaltfläche "Fertig stellen", um die Konfiguration abzuschließen.

Patchmanagement, Virenschutz und Whitelisting

Die Quarantäne-Station ist ein "Eingangstor" für Daten in das Automatisierungssystem. Über diese Station kann somit auch Schadsoftware in die Anlage gelangen. Aus diesem Grund muss diese Station in das Patchmanagement und das Virenschutzkonzept der Anlage eingebunden und einbezogen werden. D.h. die Quarantäne-Station muss regelmäßig mit den aktuellen Windows Updates versorgt werden. Als Updatequelle kann der WSUS-Server dienen, der sich auch im Perimeter-Netzwerk befindet. Des Weiteren muss auf der Quarantäne-Station ein aktueller Virenscanner installiert werden. Aktuelle Virendefinitionen erhält die Station über den Virenscanserver, der ebenfalls im Perimeter-Netzwerk platziert ist. Whitelisting ist ein weiterer Schutz, der auch bei der Quarantäne-Station implementiert werden soll (siehe hierzu die entsprechenden Kapiteln in diesem Dokument).

3.7 Konfiguration der Netzwerkkomponenten SCALANCE X

Folgende Punkte müssen bei der Konfiguration der Netzwerkkomponenten (z.B. Ethernet Switches) dringend beachtet werden:

- Deaktivierung nicht benötigter Ports
- Ändern des vorkonfigurierten Standard-Passworts (Default-Passwort)
- Deaktivierung nicht benötigter Protokolle

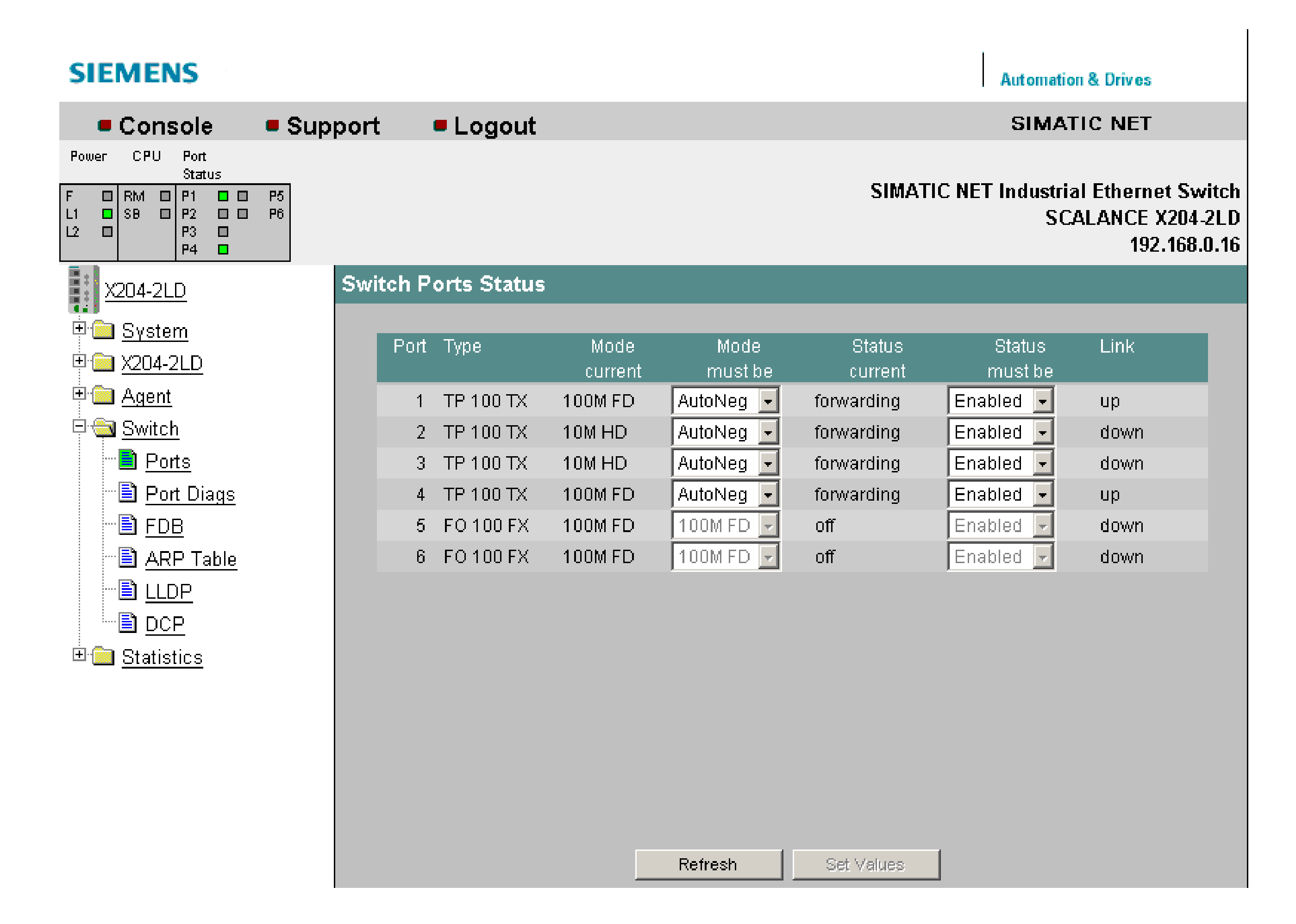
Hinweis

Zur Konfiguration der Industrial Ethernet Switches SCALANCE X beachten Sie die Betriebsanleitungen zu den entsprechenden Geräten.

Wenn Sie zum Aufbau der verschiedenen Netzwerke Switches von Fremdherstellern verwenden, beachten Sie zur Konfiguration dieser Geräte die entsprechende Betriebsanleitung des Fremdherstellers.

Deaktivierung nicht benötigter Ports

Freie Ports (Ports des Ethernet Switch), die nicht benötigt werden und an die somit keine Endgeräte angeschlossen werden, müssen deaktiviert werden. Öffnen Sie dazu das WBM-Menü "Switch Ports" und deaktivieren Sie in dieser Maske die Ports, die nicht benötigt werden.



Dieser Dialog informiert Sie über den aktuellen Zustand der Ports. Zudem können verschiedene Porteinstellungen vorgenommen werden:

- Port: Zeigt die Portnummer an.
- Type: Zeigt die Art des Ports an.
- Mode: Zeigt die Übertragungsgeschwindigkeit (10 oder 100 MBits/s) und das Übertragungsverfahren (Vollduplex oder Halbduplex) an.
- Negotiation: Zeigt an, ob Autonegotiation aktiviert oder deaktiviert ist.
- Status: Zeigt an, dass der Port eingeschaltet ist.
- Link: Zeigt den Verbindungsstatus zum Netzwerk an.

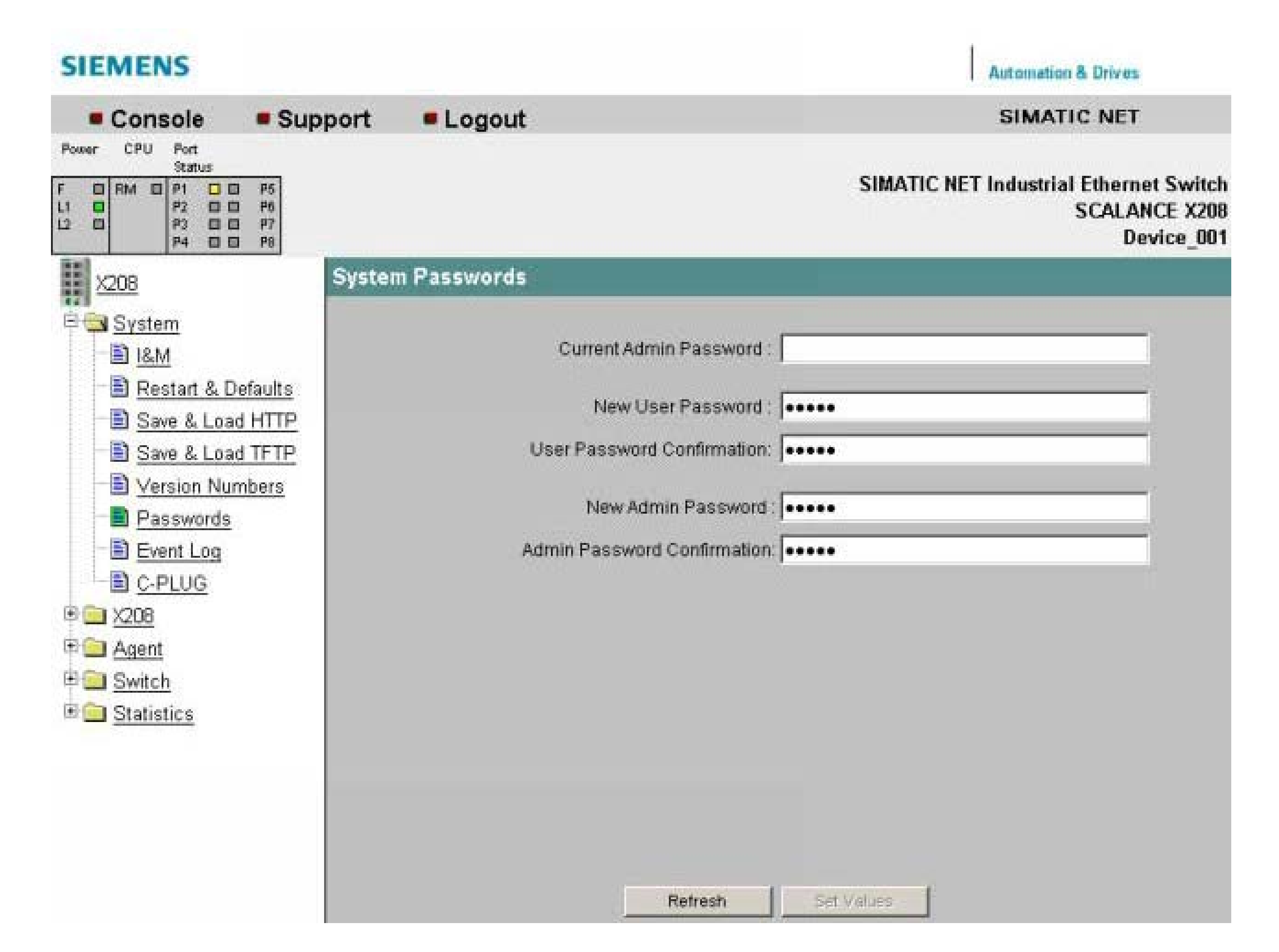
Wenn ein Port nicht verwendet wird, muss der Status dieses Ports auf "Disabled" gestellt werden.

System Passwords

Ändern Sie in der Maske "System Passwords" die Passwörter für die Benutzer "Admin" und "User". Bei Auslieferung sind die folgenden Passworte voreingestellt:

- Benutzer "User": user
- Benutzer "Admin": admin

Für die Änderung der Passwörter ist eine Anmeldung als Administrator erforderlich. Die Änderungen bestätigen Sie über die Schaltfläche "Set Value".



Deaktivierung nicht benötigter Protokolle

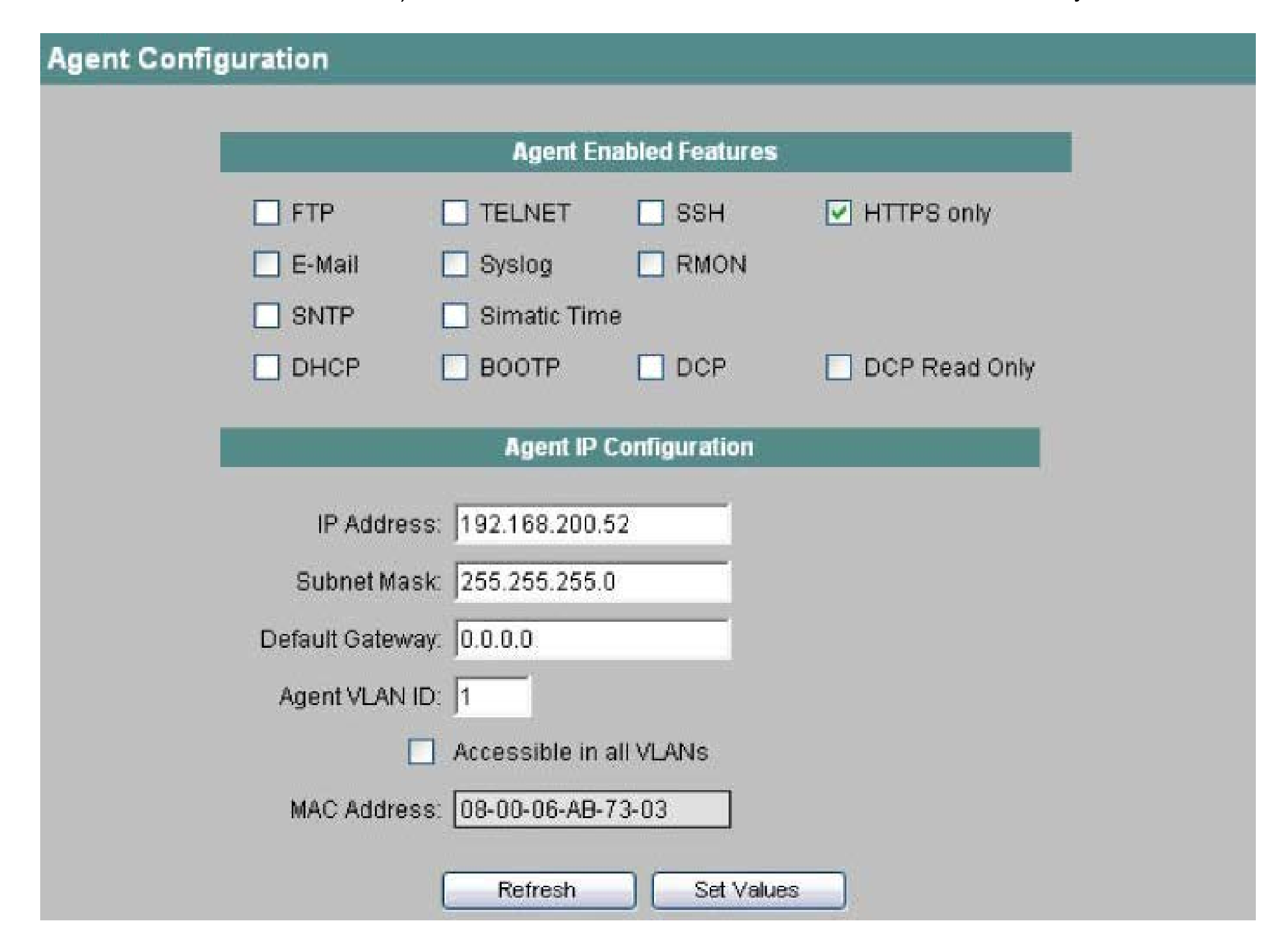
Im Dialog "Agent Configuration", der über das Ordnersymbol "Agent" geöffnet werden kann, werden u.a. die Zugriffsmöglichkeiten auf den IE-Switch festgelegt. Des Weiteren kann hier die Netzwerkkonfiguration für den IE-Switch festgelegt werden.

Verwendung statischer IP-Adressen

Beachten Sie bei dieser Einstellung, dass eine statische IP-Adresse mit einer Subnetzmaske verwendet wird. Siehe hierzu das Kapitel "Verwaltung von Netzwerken und Netzwerkdiensten" (Seite 34), Abschnitt "DHCP (Dynamic Host Configuration Protocol)".

Festlegung von Protokollen

Es wird empfohlen, für den Zugriff auf den IE-Switch, ausschließlich das Protokoll "HTTPS" festzulegen. Dazu deaktivieren Sie im Dialog "Agent Configuration" alle Protokolle (z.B. FTP, TELNET, E-Mail) und aktivieren Sie ausschließlich das Protokoll "HTTPS only".



Weitere Informationen

Weitere Informationen finden Sie in den folgenden Handbüchern:

- SIMATIC NET Industrial Ethernet Switches SCALANCE X-400 (http://support.automation.siemens.com/WW/view/de/19625108)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-300 (http://support.automation.siemens.com/WW/view/de/67480000)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-200 Projektierungshandbuch (http://support.automation.siemens.com/WW/view/de/63203259)
- SIMATIC NET Industrial Ethernet Switches SCALANCE X-200 Betriebsanleitung (http://support.automation.siemens.com/WW/view/de/63203773)

Unterstützung bei der Umsetzung bzw. Implementierung der Netzwerksicherheit in Ihrer Anlage erhalten Sie bei den Industrial Security Services. Weitere Informationen und die entsprechenden Ansprechpartner finden Sie unter http://www.industry.siemens.com/topics/global/de/industrial-security/seiten/default.aspx.

Sie können Ihre Anfrage per E-Mail auch direkt an "industrialsecurity.i@siemens.com" richten.

Systemhärtung 4

4.1 Übersicht

Quelle: https://www.bsi.bund.de

"Unter Härten (engl. Hardening) in der Informationssicherheit versteht man, die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe nicht zwingend notwendig sind."

D.h. unter Härtung sind zusammengefasst alle Maßnahmen und Einstellungen zu verstehen, mit dem Ziel

- der Reduzierung von Möglichkeiten, Verwundbarkeiten in Software auszunutzen
- der Minimierung von möglichen Angriffsmethoden
- der Beschränkung, von zur Verfügung stehenden Werkzeugen nach einem erfolgreichen Angriff
- der Minimierung, von zur Verfügung stehenden Rechten nach einem erfolgreichen Angriff
- der Erhöhung der Wahrscheinlichkeit für die Entdeckung eines erfolgreichen Angriffs

um dadurch die lokale Sicherheit und Robustheit eines Computers gegen Angriffe zu erhöhen.

Daraus ergibt sich, dass ein System dann als "gehärtet" bezeichnet werden kann, wenn:

- nur die Softwarekomponenten und Dienste installiert sind, die zum eigentlichen Betrieb benötigt werden
- ein restriktives Benutzermanagement umgesetzt ist
- die lokale Windows-Firewall aktiviert und diese restriktiv konfiguriert ist

4.2 Installation des Betriebssystems

Einleitung

Das Betriebssystem und die SIMATIC PCS 7-Software sind auf den SIMATIC PCS 7 Industrial Workstation (IPC) bereits vorinstalliert.

Hinweis

Bei einer manuellen Durchführung der Installation beachten Sie die in den folgenden Dokumenten beschriebenen Voraussetzungen und Vorgehensweisen:

- PCS 7 Liesmich (http://support.automation.siemens.com/WW/view/de/66807356)
- Handbuch "SIMATIC Prozessleitsystem PCS 7 PC-Konfiguration und Autorisierung" (http://support.automation.siemens.com/WW/view/de/68157327)

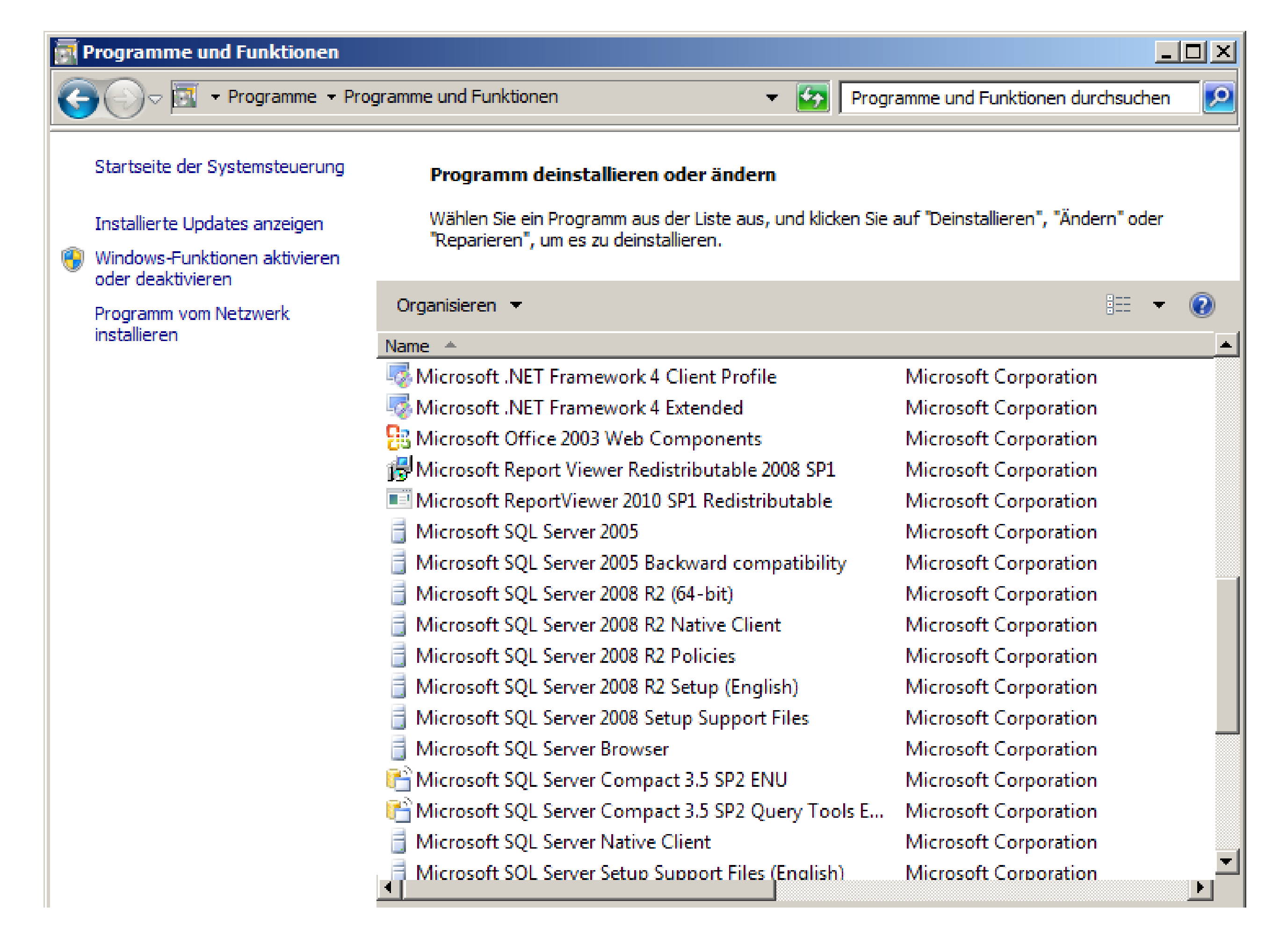
Für einen SIMATIC PCS 7 Rechner, der in einer Automatisierungsanlage eine bestimmte Funktion erfüllt (OS-Server, OS-Client, Engineering Station) sind bestimmte Programme, die durch die Installation des Betriebssystems installiert wurden, nicht notwendig. Diese Programme sollen deinstalliert werden. Hierbei handelt es sich in den meisten Fällen um "Windows-Komponenten" z.B. Spiele, Rechner, Notepad, WordPad, Paint usw.

Deinstallieren von Windows-Komponenten

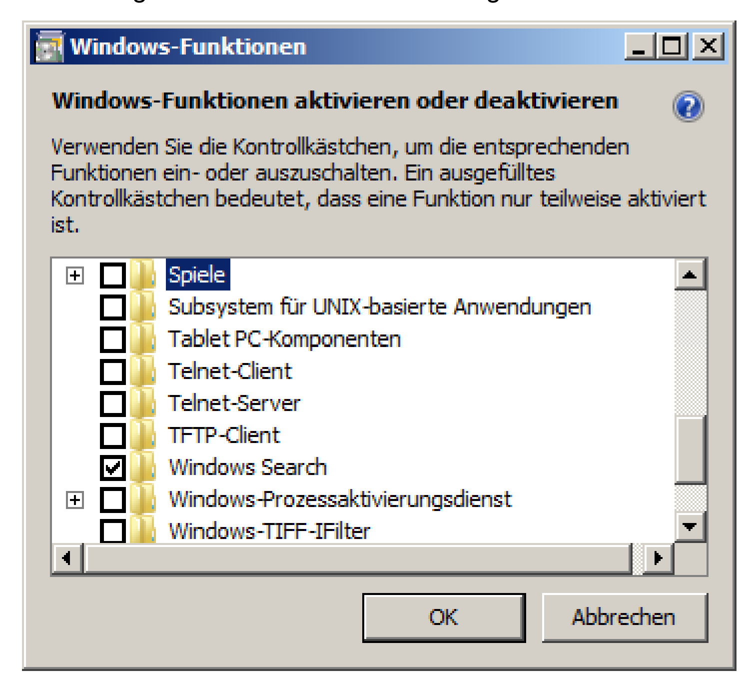
Die folgende Vorgehensweise wird am Beispiel des Betriebssystems "Windows 7" beschrieben.

Um nicht benötigte Windows-Komponenten zu deinstallieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Windows-Startmenü den Befehl "Start > Systemsteuerung > Programme > Programme und Funktionen".
   Der Dialog "Programme deinstallieren oder ändern" wird geöffnet.



2. Klicken Sie im Navigationsbereich auf den Eintrag "Windows-Funktionen aktivieren oder deaktivieren".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie bereits als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Dialog "Windows-Funktionen" wird geöffnet.



3. Deaktivieren Sie die nicht benötigten Komponenten.
4. Bestätigen Sie die Änderungen mit der Schaltfläche "OK".

Deaktivieren von Diensten

Entsprechend den Vorgaben zur Härtung eines Systems sollen neben den Softwarepaketen, die für den Betrieb eines Systems nicht notwendig sind, auch die nicht benötigten Dienste deaktiviert werden.

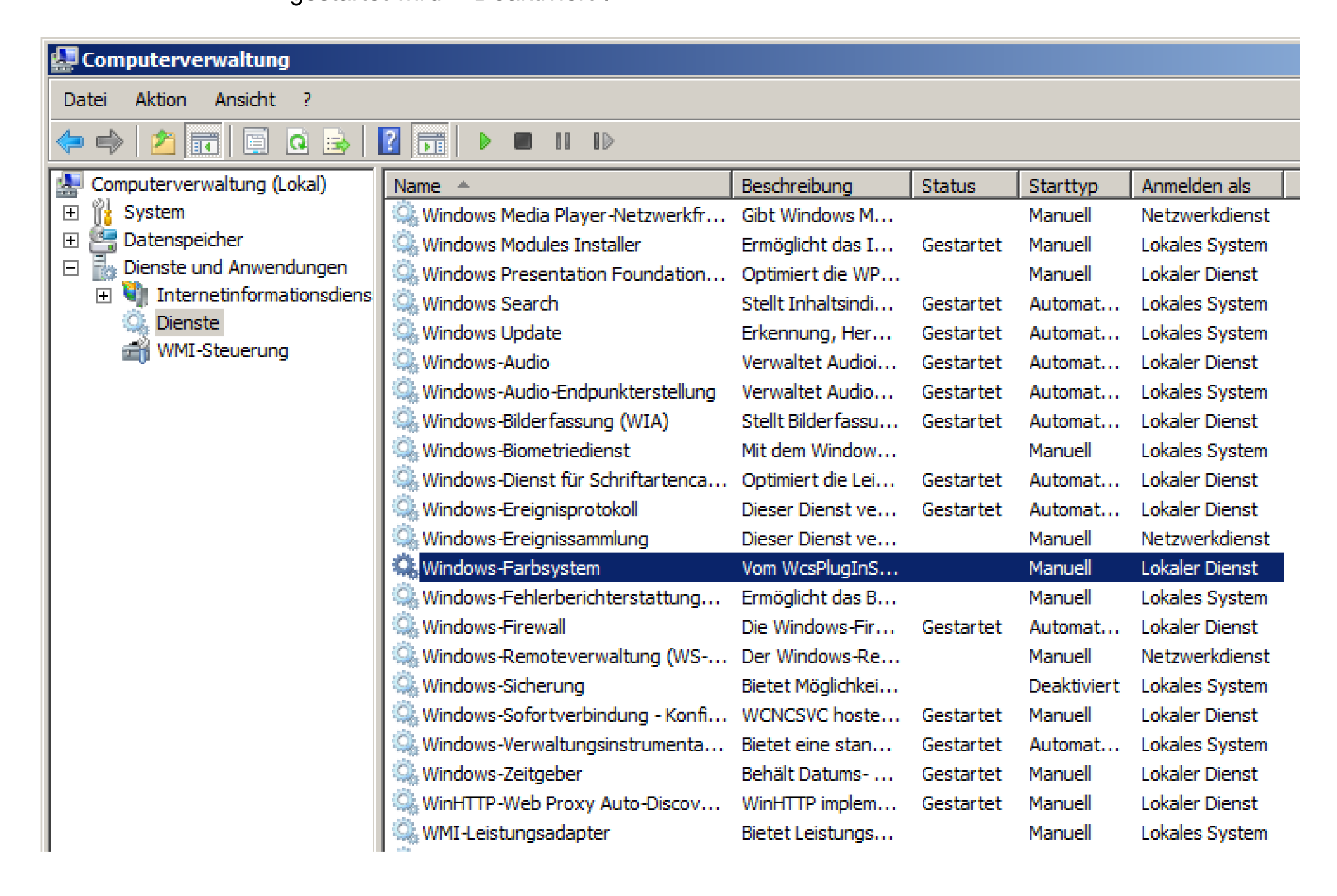
Folgende Dienste können deaktiviert werden:

Dienst	Betriebssystem
Zertifikatverteilung	Windows 7, Windows Server 2008 R2
Diagnoserichtliniendienst	Windows 7, Windows Server 2008 R2
Diagnosediensthost	Windows 7, Windows Server 2008 R2
Windows-Farbsystem	Windows 7, Windows Server 2008 R2
Windows-Sofortverbindung - Konfigurationsregistrierungsstelle	Windows 7
Leistungsprotokolle und -warnungen	Alle
Windows Presentation Foundation-Schriftartcache	Alle
Hilfe und Support	Windows XP, Windows Server 2003 R2
Konfigurationsfreie drahtlose Verbindung	Windows XP, Windows Server 2003 R2
Terminaldienste-Sitzungsverzeichnis	Windows Server 2003 R2

Vorgehensweise

Um einen Dienst zu deaktivieren, gehen Sie folgendermaßen vor:

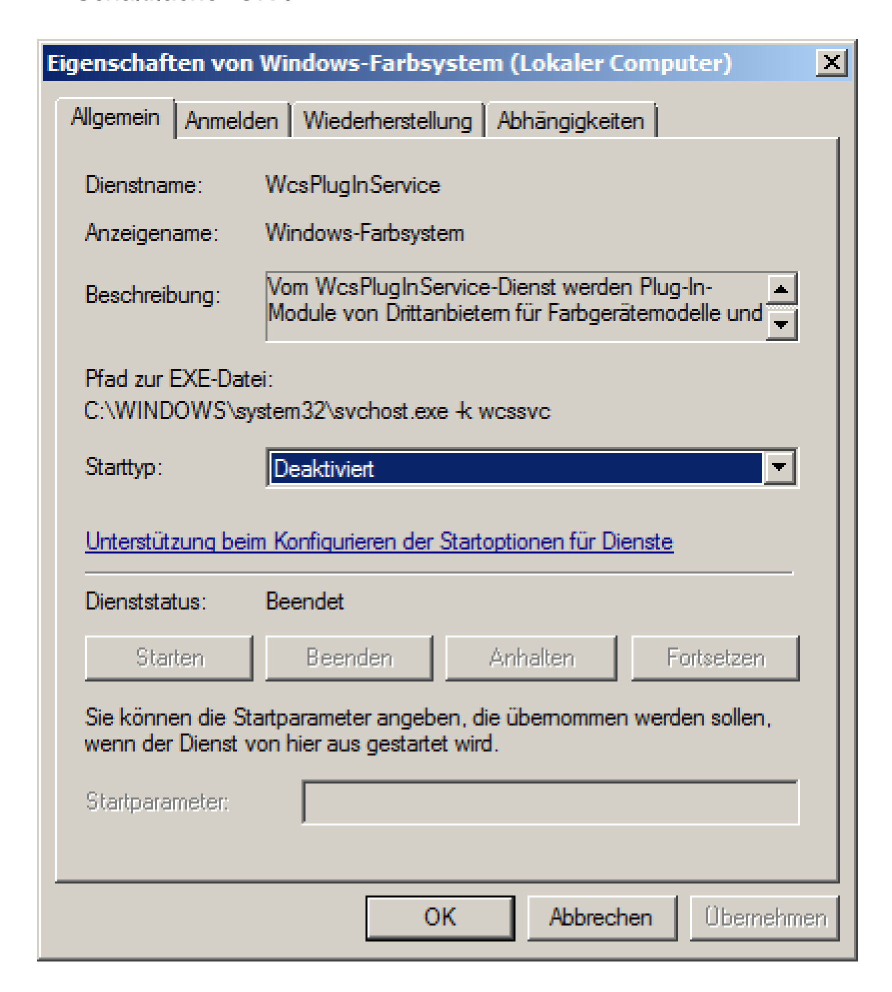
1. Klicken Sie im Windows Start-Menü mit der rechten Maustaste auf "Computer" und wählen Sie im Kontextmenü den Befehl "Verwalten".
   Geben Sie das Administratorenpasswort ein, falls dies erforderlich ist. Wenn Sie bereits als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Dialog "Computerverwaltung" wird geöffnet.
2. Wählen Sie im Navigationsbereich den Eintrag "Dienste und Anwendungen > Dienste".
   Im rechten Bereich des Dialogs werden alle verfügbaren Dienste angezeigt. Die Spalte "Status" zeigt, ob der Dienst aktuell gestartet ist. In der Spalte "Starttyp" wird angezeigt, wie der Dienst gestartet wird - "Manuell" oder "Automatisch" oder ob der Dienst nicht gestartet wird - "Deaktiviert".



3. Selektieren Sie im rechten Bereich den Dienst, den Sie deaktivieren möchten und öffnen durch Doppelklick den Eigenschaftendialog des Dienstes.
4. Klicken Sie auf die Schaltfläche "Beenden", um den Dienst zu beenden.



5. Wählen Sie als Starttyp "Deaktiviert" und bestätigen Sie die Änderungen durch die Schaltfläche "OK".



4.3 Security Controller

Der Security Controller (ab PCS 7 V8.0) bzw. das SIMATIC Security Control (<PCS 7 V8.0) ist ein Programm, das anwendungsspezifische Sicherheitseinstellungen vornimmt. In SIMATIC PCS 7 und SIMATIC WinCC ist der Security Controller (SC) bzw. das SIMATIC Security Control (SSC) standardmäßig integriert.

Die Option, dass der SC die Einstellungen automatisch ausführen darf, muss bei der Installation der Programme explizit bestätigt werden.

Die Kommunikation zu nicht konfigurierten Geräten oder zu anderen Subnetzen sowie die Nutzung durch nicht konfigurierte Benutzer sind nicht möglich oder stark eingeschränkt.

Bei einer Änderung des Anlagenaufbaus oder einer Änderung der Zuständigkeit von Benutzern ist zu beachten, dass die lokale Firewall-Konfiguration bzw. die lokalen Gruppenmitgliedschaften angepasst werden müssen.

Durch den Security Controller werden die folgenden Einstellungen automatisch vorgenommen:

- Group Settings (Benutzerverwaltung – SIMATIC Logon)
- Registry Settings
- Windows Firewall Exceptions
- DCOM Settings
- File and/or Directory Permissions

Diese Einstellungen werden in Abhängigkeit von der Installation (PCS 7 OS-Server, PCS 7 OS-Client, ES) und für folgende Software-Pakete vorgenommen:

- Automation License Manager
- File and Printer Sharing
- SIMATIC Batch
- SIMATIC Communication Services
- SIMATIC Logon
- SIMATIC Management Console
- SIMATIC NET PC-Software
- SIMATIC PC Diagnosis Application
- SIMATIC PCS 7 Engineering System
- SIMATIC Route Control
- SIMATIC SFC Visualization (SFV)
- SIMATIC STEP 7 Components
- SIMATIC WinCC
- SIMATIC WinCC OPC
- SIMATIC WinCC User Archive
- SQL Server (Version des SQL-Servers ist abhängig von der SIMATIC PCS 7 Version)

Hinweis

Beachten Sie auch die Informationen im Handbuch "SIMATIC Prozessleitsystem PCS 7 PC-Konfiguration und Autorisierung" (http://support.automation.siemens.com/WW/view/de/68157327).

4.4 Windows Firewall

Einleitung

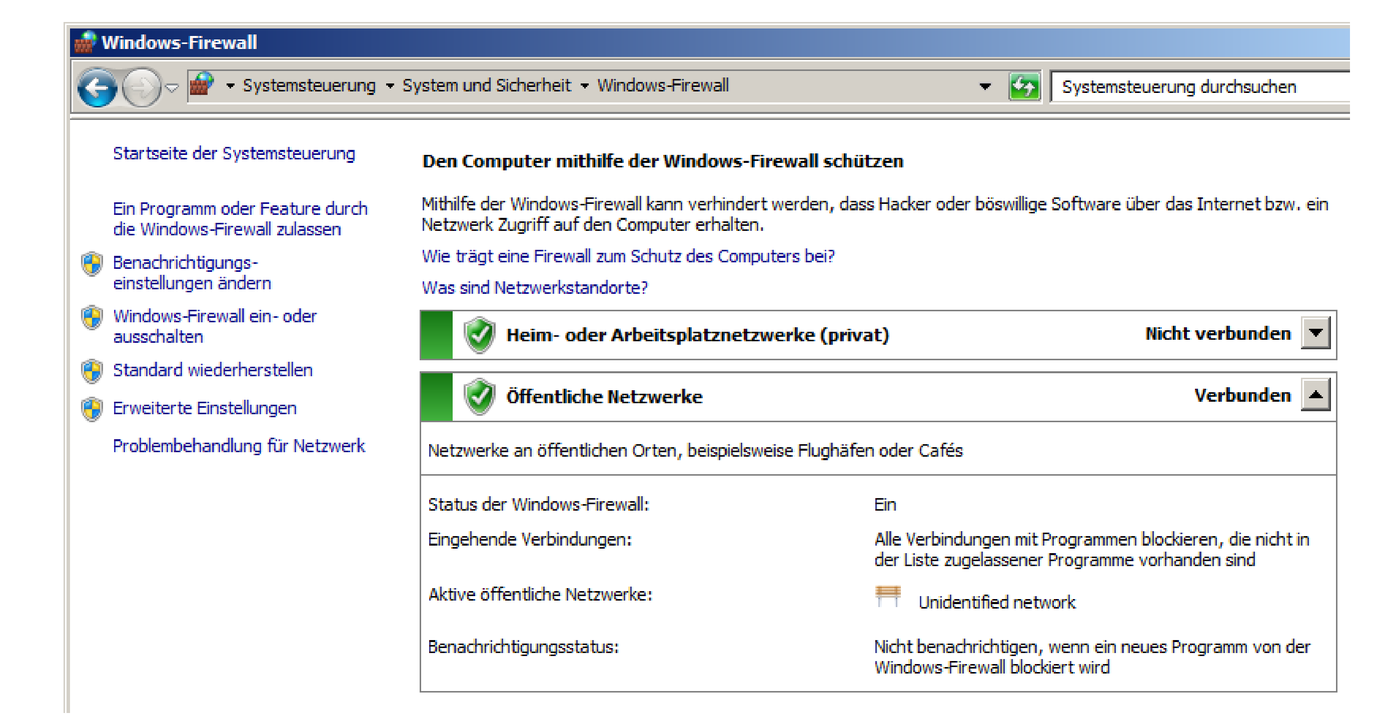
Wie im Kapitel "Security Controller" (Seite 71) beschrieben, nimmt der Security Controller (ab PCS 7 V8.0) bzw. das SIMATIC Security Control (<PCS 7 V8.0) Einstellungen in Bezug auf die Windows Firewall vor. In Hinsicht auf die Musterkonfiguration, bei der eine Kommunikation von PCS 7 Rechnern zwischen unterschiedlichen Subnetzen gewährleistet sein muss, ist es notwendig, manuelle Anpassungen an der Windows Firewall vorzunehmen.

Musterkonfiguration: Windows Firewall

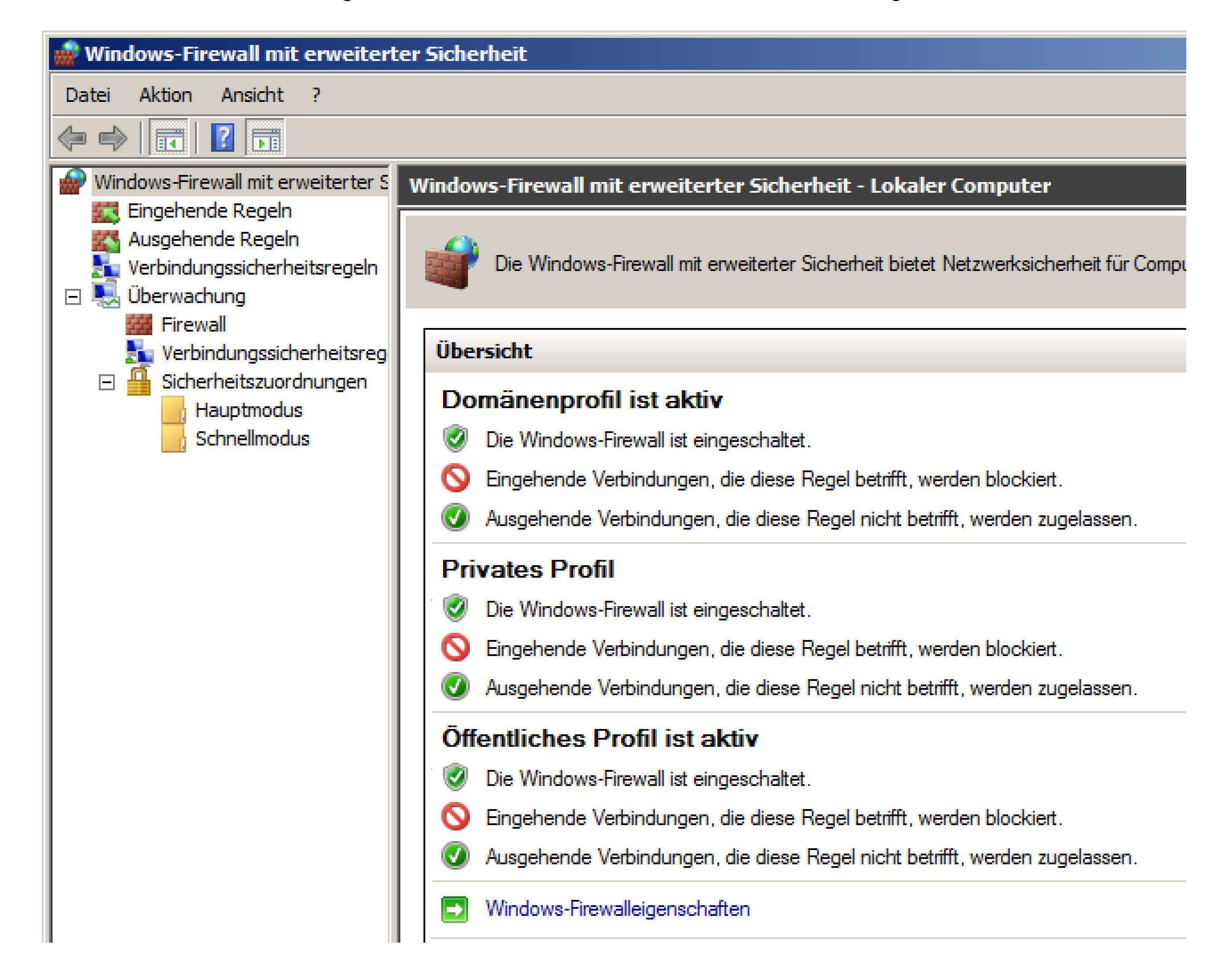
Die folgende Vorgehensweise wird am Bespiel des Betriebssystems "Windows 7" beschrieben.

Damit die Kommunikation beispielsweise zwischen dem OS Web Server mit der IP-Adresse 192.168.2.203 und dem OS-Server OSS1A mit der IP-Adresse 192.168.2.101, die sich in unterschiedlichen Subnetzen befinden (Perimeter-Netzwerk und PCN1), nicht von der Windows Firewall blockiert wird, muss folgende Anpassung in der Windows Firewall bzw. in den Firewall-Regeln gemacht werden:

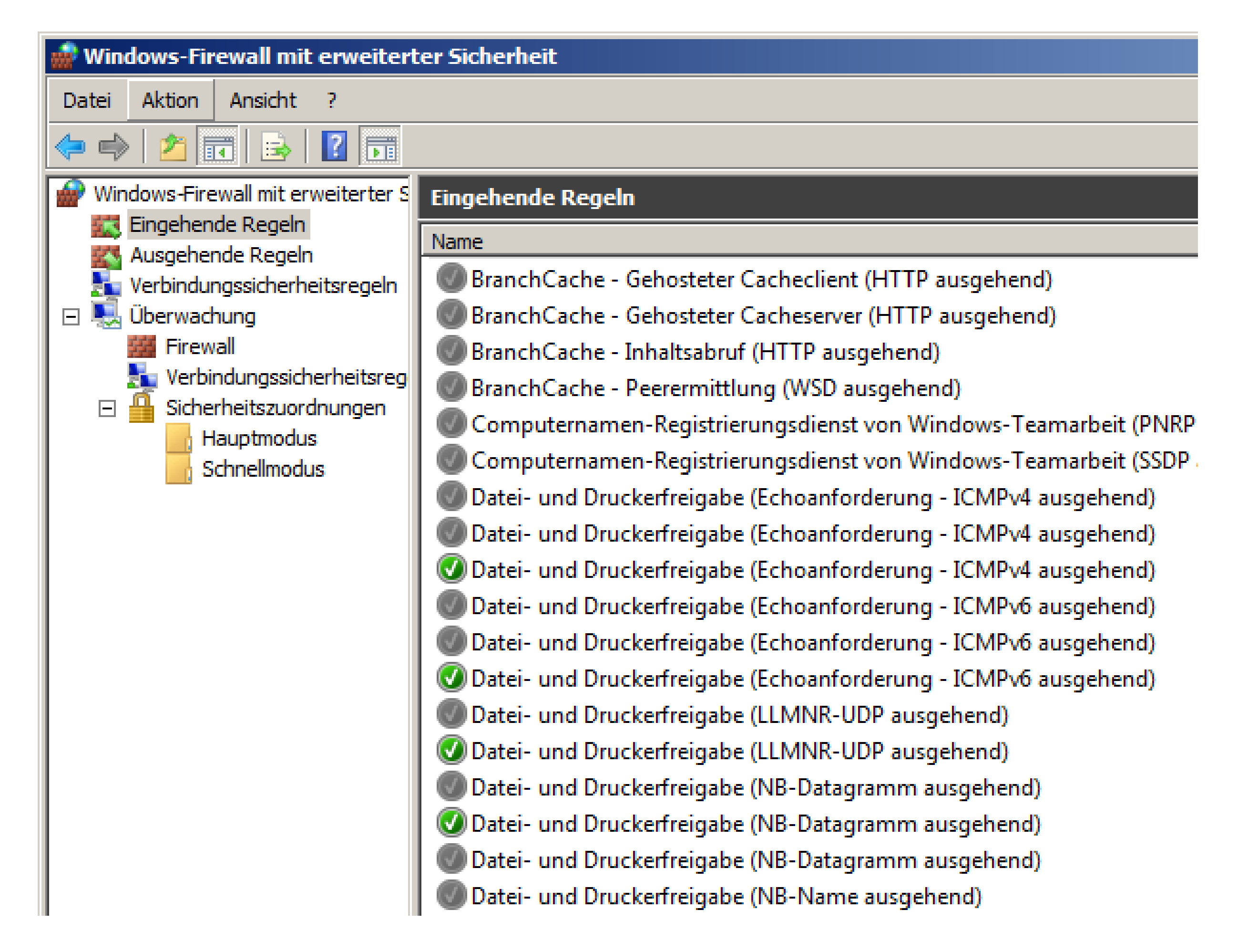
1. Öffnen Sie die Windows-Firewall über den Befehl "Start > Systemsteuerung > System und Sicherheit > Windows -Firewall".
   Der Dialog "Windows-Firewall" wird geöffnet.



2. Klicken Sie im linken Navigationsbereich auf "Erweiterte Einstellungen".
   Geben Sie das Administratorenpasswort, falls dies erforderlich ist. Wenn Sie als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Dialog "Windows-Firewall mit erweiterter Sicherheit" wird geöffnet.

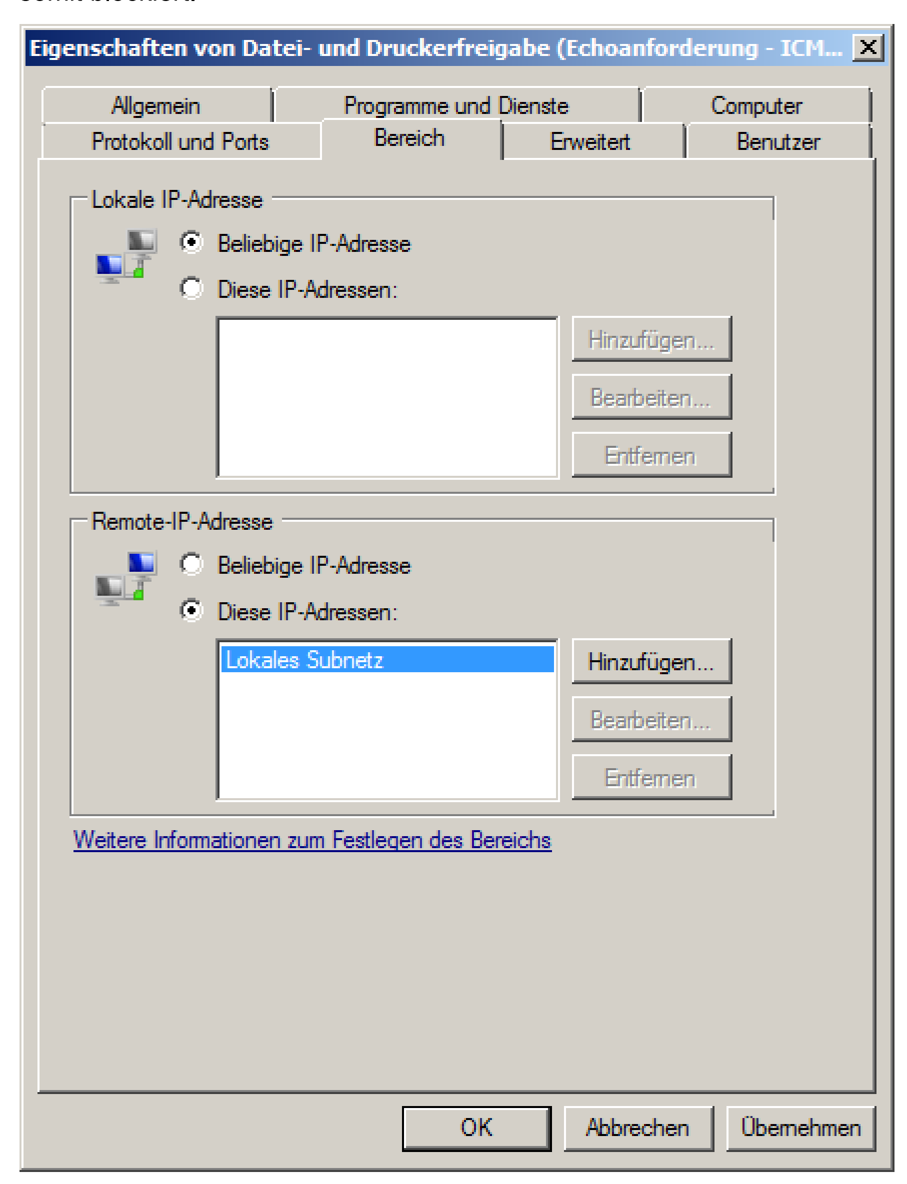


3. Klicken Sie im linken Navigationsbereich auf "Eingehende Regeln".
   Die "Eingehende Regeln" werden angezeigt.

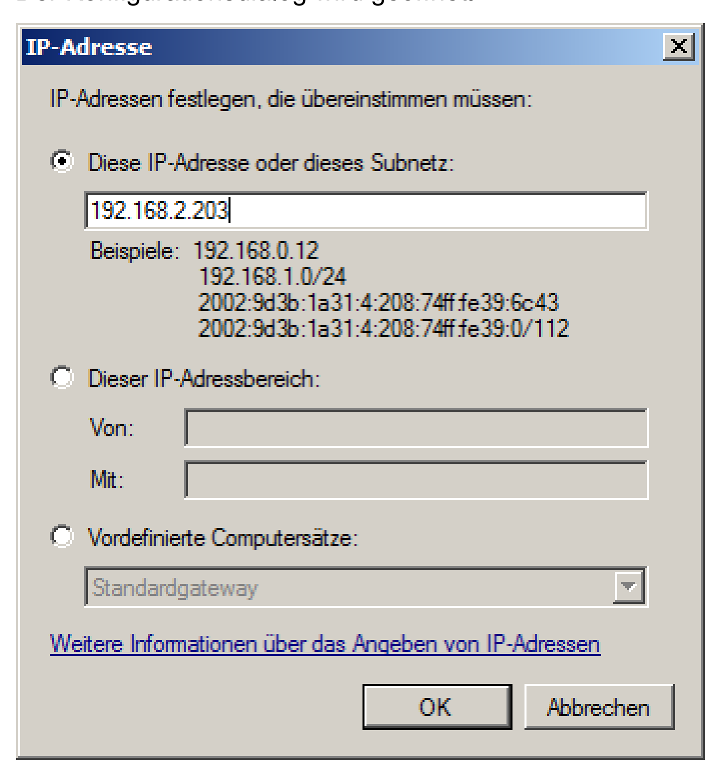


4. Öffnen Sie die Eigenschaften einer aktiven Datei- und Druckerfreigabe Regel durch Doppelklick.
   Der Eigenschaftsdialog dieser Regel wird geöffnet.

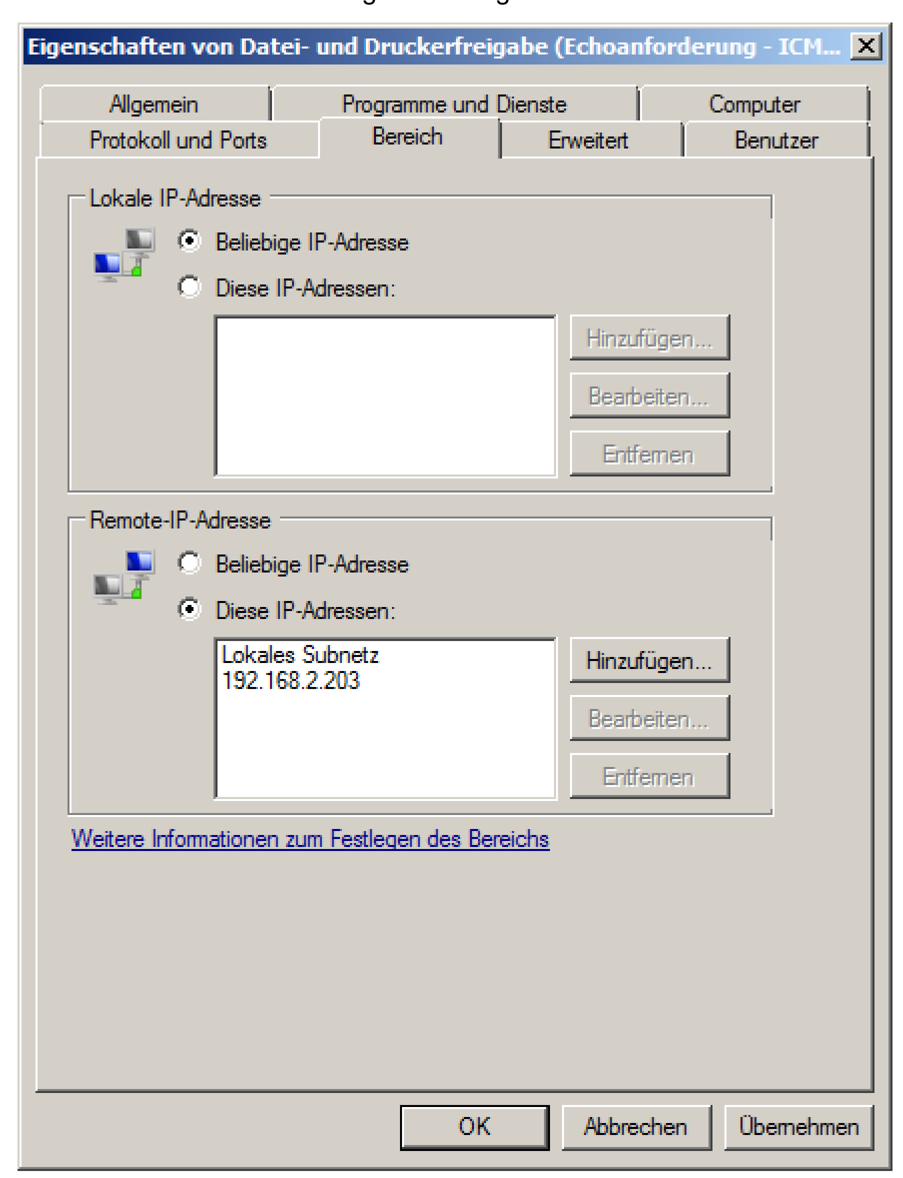
5. Öffnen Sie das Register "Bereich".
   Im Bereich "Remote-IP-Adresse" wird der IP-Adressbereich angezeigt, für den diese Firewall-Regel die ankommende Kommunikation nicht blockiert.
   Im Fall der folgenden Abbildung wird die Kommunikation nur mit Computern im "Lokalen Subnetz" erlaubt. Eine Kommunikation zu Computern in einem anderen Subnetz wird somit blockiert.



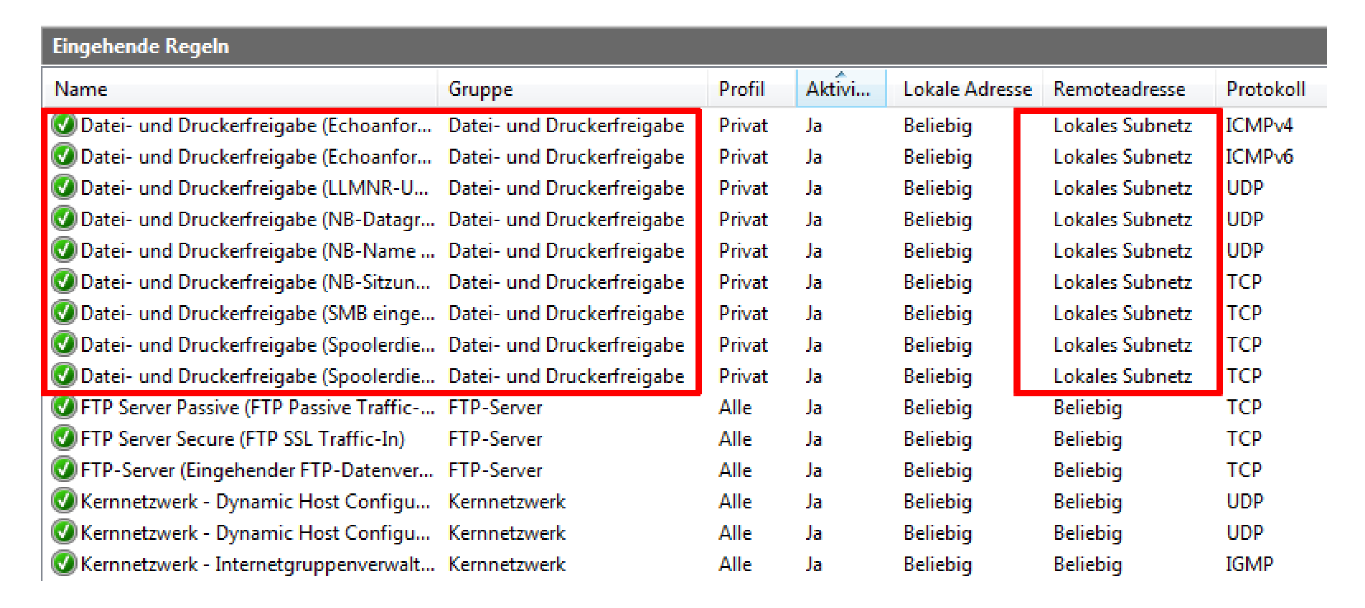
6. Um die Kommunikation des OS-Servers "OSS1A" zum OS Web Server mit der IP-Adresse 192.168.2.203 im Subnetz "Perimeter-Netzwerk" zu erlauben, klicken Sie im Bereich "Remote IP-Adresse" auf die Schaltfläche "Hinzufügen".
   Der Konfigurationsdialog wird geöffnet.



7. Wählen Sie die Option "Diese IP-Adresse oder dieses Subnetz:" und tragen Sie die IP-Adresse des Kommunikationspartners ein. Wenn Sie die Fire Wall-Regeln am OS-Server "OSS1A" konfigurieren, geben Sie in diesem Dialog die IP-Adresse des OS Web Servers 192.168.2.203 an und bestätigen die Eingabe mit der Schaltfläche "OK".



8. Bestätigen Sie die Änderung mit der Schaltfläche "OK".
9. Passen Sie alle eingehenden und ausgehenden Regeln entsprechend an.



Eingehende Regeln

Name	Gruppe	Profil	Aktivi...	Lokale Adresse	Remoteadresse	Protokoll
Datei- und Druckerfreigabe (Echoanfor...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	ICMPv4
Datei- und Druckerfreigabe (Echoanfor...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	ICMPv6
Datei- und Druckerfreigabe (LLMNR-U...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	UDP
Datei- und Druckerfreigabe (NB-Datagr...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	UDP
Datei- und Druckerfreigabe (NB-Name ...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	UDP
Datei- und Druckerfreigabe (NB-Sitzun...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	TCP
Datei- und Druckerfreigabe (SMB einge...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	TCP
Datei- und Druckerfreigabe (Spoolerdie...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	TCP
Datei- und Druckerfreigabe (Spoolerdie...	Datei- und Druckerfreigabe	Privat	Ja	Beliebig	Lokales Subnetz	TCP
FTP Server Passive (FTP Passive Traffic-...	FTP-Server	Alle	Ja	Beliebig	Beliebig	TCP
FTP Server Secure (FTP SSL Traffic-In)	FTP-Server	Alle	Ja	Beliebig	Beliebig	TCP
FTP-Server (Eingehender FTP-Datenver...	FTP-Server	Alle	Ja	Beliebig	Beliebig	TCP
Kernnetzwerk - Dynamic Host Configu...	Kernnetzwerk	Alle	Ja	Beliebig	Beliebig	UDP
Kernnetzwerk - Dynamic Host Configu...	Kernnetzwerk	Alle	Ja	Beliebig	Beliebig	UDP
Kernnetzwerk - Internetgruppenverwalt...	Kernnetzwerk	Alle	Ja	Beliebig	Beliebig	IGMP

4.5 BIOS-Einstellungen

Die folgenden BIOS-Einstellungen müssen Sie auf jedem Rechner Ihrer Anlage durchführen:

- Der Zugang zum BIOS muss mit einem Passwort geschützt werden. Das Passwort muss von einem Administrator festgelegt und vertraulich behandelt werden.
- Die Start-Reihenfolge des Rechners muss im BIOS so eingestellt sein, dass von der Festplatte gestartet wird. Dies bedeutet, dass die Festplatte als erstes Start-Medium eingestellt werden muss. Dadurch wird das Starten von anderen Medien, z.B. von CD oder USB erschwert.
- Die Reihenfolge, in der die einzelnen Medien des Rechners gestartet werden, muss im BIOS so eingestellt werden, dass die Festplatte als erstes gestartet wird. Dadurch wird das Starten von anderen Medien, z. B. von CD oder USB erschwert.
- Die USB-Ports müssen, wenn sie nicht für Peripherie-Geräte wie z. B. Maus oder Tastatur benötigt werden, deaktiviert (disabled) werden.

Hinweis

Die Einstellungen für einen speziellen Rechner hängen vom installierten BIOS (z. B. Hersteller, Version) ab. Entnehmen Sie die spezifischen Möglichkeiten der Einstellung der entsprechenden Systembeschreibung.

4.6 Umgang mit mobilen Datenträgern

4.6.1 Übersicht

Einleitung

Neben der Abgrenzung und Nennung mobiler Datenträger werden in diesem Kapitel Hinweise gegeben, welche Einstellungen in Bezug auf mobile Datenträger vorzunehmen sind.

Mobile Datenträger

Quelle:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05014.html

Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern, hierzu gehören unter anderem Disketten, Wechselplatten, CD-/DVDs, USB-Festplatten und auch Flash-Speicher wie USB-Sticks. Durch diese Vielzahl an Formen und Einsatzgebieten werden nicht immer alle erforderlichen Sicherheitsbetrachtungen vorgenommen.

Mobile Datenträger können eingesetzt werden für

- den Datenaustausch,
- den Datentransport zwischen IT-Systemen, die nicht miteinander vernetzt sind, oder zwischen verschiedenen Orten,
- die Archivierung oder Speicherung von Sicherheitskopien (Backup), falls andere automatisierte Verfahren nicht zweckmäßig sind,
- die Speicherung von Daten, die zu sensitiv sind, um sie auf Arbeitsplatzrechnern oder Servern zu speichern,
- die mobile Datennutzung oder Datenerzeugung (z. B. MP3-Player, Digitalkamera, etc.).

Abgrenzung USB-Speichermedien

Quelle:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04200.html

Über die USB-Schnittstelle lassen sich eine Vielzahl von Zusatzgeräten an PCs anschließen. Beispiele sind Festplatten, CD / DVD -Brenner und Memory-Sticks. USB-Memory-Sticks bestehen aus einem USB-Stecker und einem Speicherchip. Trotz großer Speicherkapazität sind sie so handlich, dass sie beispielsweise in Form von Schlüsselanhängern hergestellt werden und in jede Hosentasche passen. In modernen Betriebssystemen sind die Treiber für USB-Massenspeichergeräte bereits integriert, so dass zum Betrieb keine Softwareinstallation mehr notwendig ist. Im Allgemeinen bezieht sich diese Maßnahme nicht ausschließlich auf USB-Speichermedien, sondern generell auf alle USB-Geräte, die Daten speichern können. Unter anderem können auch USB-Drucker und USB-Kameras zum Speichern der Daten "missbraucht" werden. Dies gilt insbesondere für "intelligente" USB-Geräte wie PDAs, die jede beliebige USB-Identität annehmen können, wenn sie mit spezieller Software ausgestattet sind.

Userzugriffe auf USB-Ports einschränken

Quelle:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04200.html

Ähnlich wie über Disketten können über USB-Speichermedien unkontrolliert Informationen und Programme ein- oder ausgelesen werden. Daher ist mit USB-Speichermedien generell genauso wie mit herkömmlichen Speichermedien umzugehen. Der Zugriff auf Diskettenlaufwerke kann relativ einfach verhindert werden. Der Betrieb von USB-Speichermedien lässt sich dagegen nur sehr schwer verhindern, wenn die USB-Schnittstelle für andere Geräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Deswegen ist es meist nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren. Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden.

Umgang mit USB-Ports

Neben der BIOS-Einstellungen für die Sperrung der USB-Ports (siehe Kapitel “Auto-Hotspot“) kann der ungewünschte Zugriff auch durch Windows-Einstellungen einschränkt werden. Durch die Sperrung der USB-Ports über die BIOS-Einstellungen bzw. das Hardware-Profil wird gesichert, dass das Verbotes der unbefugten Verwendung von USB-Speichermedien eingehalten wird.

Einschränkung des Zugriffs auf USB-Speichermedien mit Hilfe von Windows

Im Folgenden werden verschiedene Vorgehensweisen beschrieben, die zeigen, wie mit Windows-Mitteln der Zugriff auf USB-Speichermedien verhindert bzw. eingeschränkt werden kann:

- Einschränkung des Zugriffs auf USB-Speichermedien mit Hilfe von Windows XP bzw. Windows Server 2003 Bordmitteln
  - Wenn noch kein USB-Speichermedium installiert ist
  - Wenn bereits ein USB-Speichermedium installiert ist
- Sperren des Zugriffs auf USB-Speichermedien mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008
- Reglementierung der Nutzung von auf USB-Speichermedien mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008
- Deaktivieren der AutoPlay-Funktion mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008
- Deaktivieren aller AutoRun-Funktionen mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008
- Deaktivieren der AutoPlay-Funktion mittels Gruppenrichtlinie in Windows XP und Windows Server 2003

4.6.2 Einschränkung des Zugriffs mit Hilfe von Windows XP bzw. Windows Server 2003 Bordmitteln

Um zu verhindern, dass ein Benutzer eine Verbindung zu einem USB-Speichermedium herstellen kann, gibt es zwei Vorgehensweisen:

- Wenn kein USB-Speichermedium auf dem Rechner installiert ist
- Wenn ein USB-Speichermedium auf dem Rechner installiert ist

Einschränkung des Zugriffs, wenn kein USB-Speichermedium auf dem Rechner installiert ist

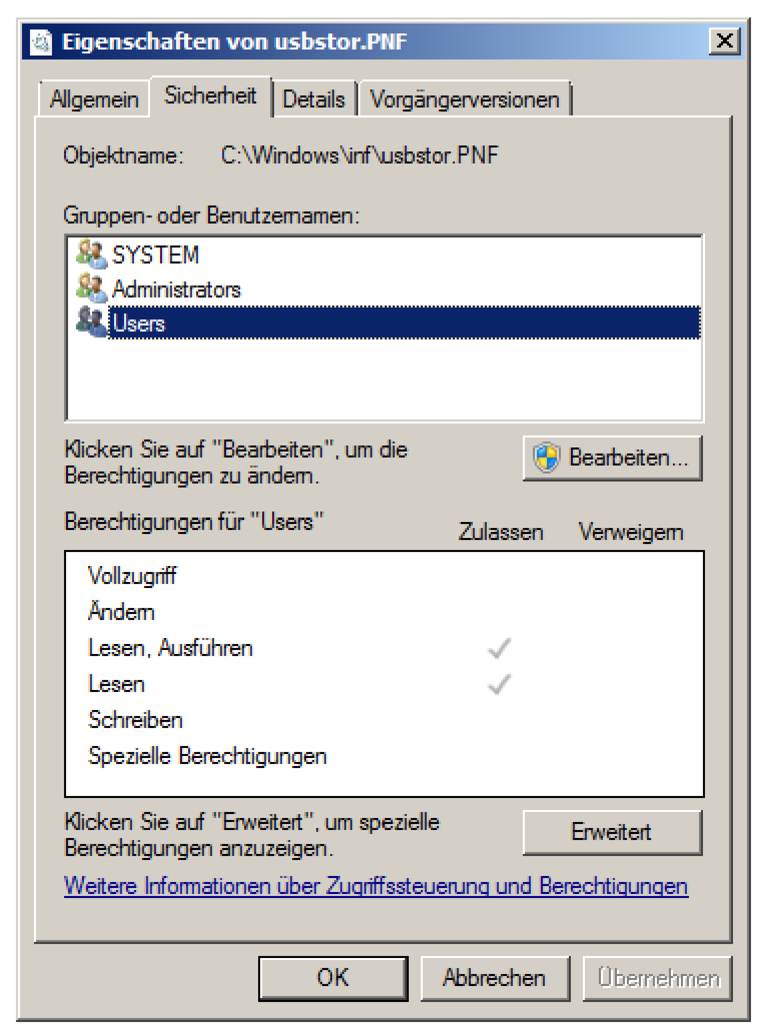
Quelle: http://support.microsoft.com/kb/823732/de

Wenn noch kein USB-Speichmedium auf dem Rechner installiert ist, weisen Sie dem Benutzer oder der Gruppe und dem lokalen Systemkonto für folgende Dateien Zugriffsverweigerungen zu:

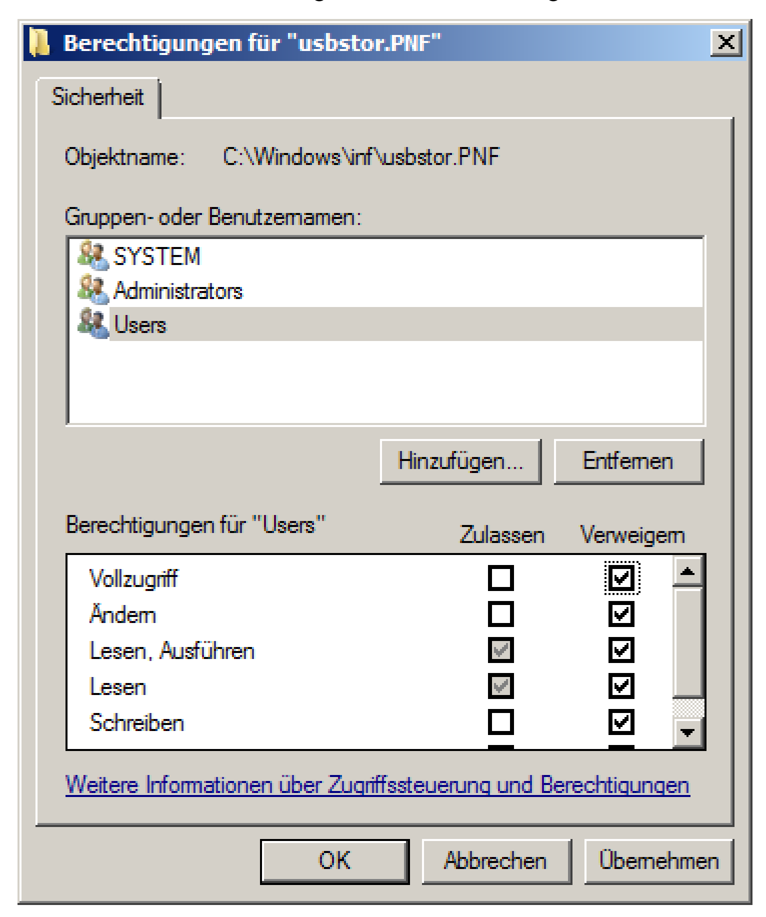
- %SystemRoot%\Inf\Usbstor.pnf
- %SystemRoot%\Inf\Usbstor.inf

Benutzer können anschließend kein USB-Speichmedium mehr auf dem Rechner installieren. Gehen Sie folgendermaßen vor, um einem Benutzer oder einer Gruppe Zugriffsverweigerungen für die Dateien Usbstor.pnf und Usbstor.inf zuzuweisen:

1. Starten Sie den Windows Explorer und suchen Sie anschließend nach dem Ordner "%SystemRoot%\Inf".
2. Klicken Sie mit der rechten Maustaste auf die Datei "Usbstor.pnf" und klicken Sie anschließend auf "Eigenschaften".
3. Klicken Sie auf die Registerkarte "Sicherheit".



4. Fügen Sie den Benutzer oder die Gruppe, für den bzw. für die Sie Zugriffsverweigerungen festlegen möchten, zur Liste Gruppen- oder Benutzernamen hinzu.
5. Aktivieren Sie in der Liste "Berechtigungen für Benutzer- oder Gruppenname" das Kontrollkästchen "Verweigern" neben "Vollzugriff".



6. Fügen Sie zusätzlich auch das Systemkonto zur Liste Verweigern hinzu. Wählen Sie dafür in der Liste "Gruppen- oder Benutzernamen" das Systemkonto "SYSTEM" aus und aktivieren Sie in der Liste "Berechtigungen für SYSTEM" das Kontrollkästchen "Verweigern" neben "Vollzugriff". Klicken Sie anschließend auf OK.
7. Wiederholen Sie die Schritte 1 - 6 ebenfalls für die Datei "Usbstor.inf".

Einschränkung des Zugriffs, wenn ein USB-Speichermedium auf dem Rechner installiert ist

Quelle: http://support.microsoft.com/kb/823732/de

ACHTUNG
Bearbeiten der Registrierung Dieser Abschnitt bzw. die Methoden- oder Aufgabenbeschreibung enthält Hinweise zum Bearbeiten der Registrierung. Durch die falsche Bearbeitung der Registrierung können schwerwiegende Probleme verursacht werden. Daher ist es wichtig, bei der Ausführung der folgenden Schritte sorgfältig vorzugehen. Als Schutzmaßnahme sollten Sie vor der Bearbeitung der Registrierung eine Sicherungskopie erstellen. So ist gewährleistet, dass Sie die Registrierung wiederherstellen können, falls ein Problem auftritt.

Wenn bereits ein USB-Speichermedium auf dem Rechner installiert ist, können Sie die Registrierung ändern, um sicherzustellen, dass das Gerät nicht funktioniert, wenn der Benutzer es an den Rechner anschließt.

Wenn bereits ein USB-Speichermedium auf dem Rechner installiert ist, setzen Sie den Wert "Start" in folgendem Registrierungsschlüssel auf den Wert 4:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor`

Dies hat zur Folge, dass das USB-Speichermedium nicht funktioniert, wenn der Benutzer das Gerät an den Rechner anschließt.

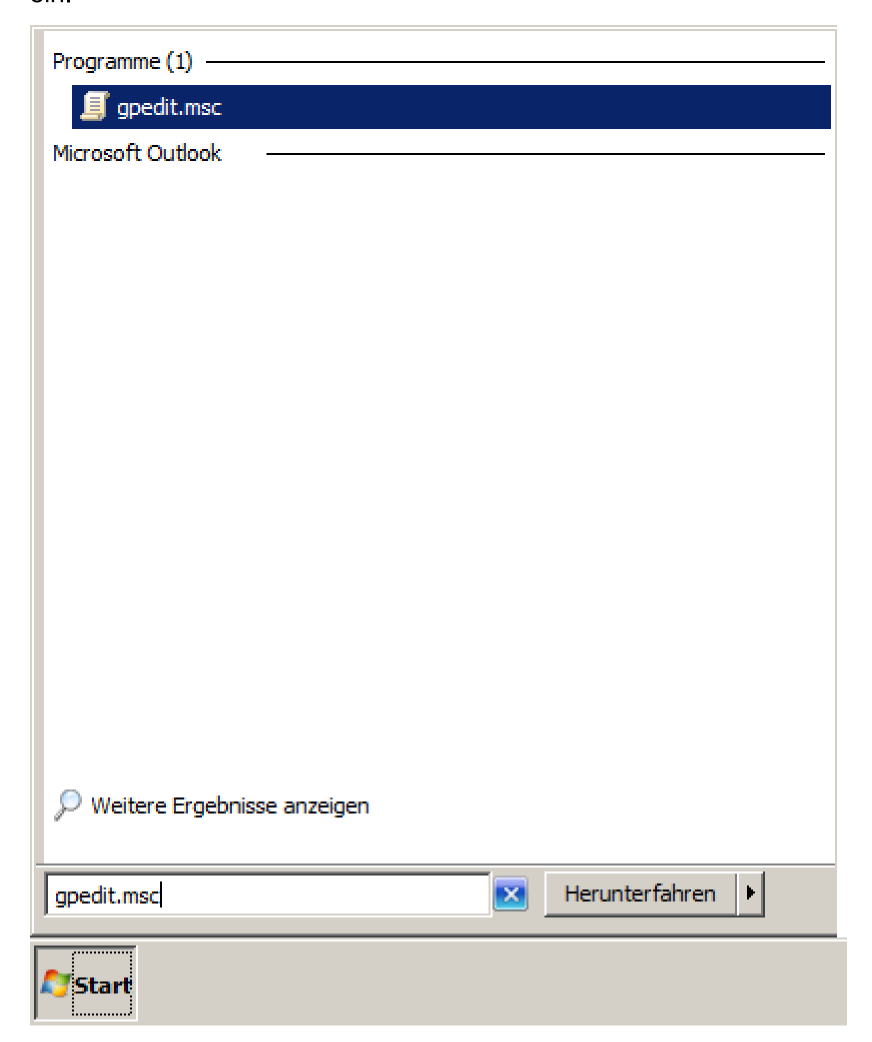
Gehen Sie folgendermaßen vor, um den Wert "Start" festzulegen:

1. Klicken Sie auf "Start" und anschließend auf "Ausführen".
2. Geben Sie in das Feld "Öffnen" die Zeichenfolge "regedit" ein, und klicken Sie auf OK.
3. Klicken Sie auf folgenden Registrierungsschlüssel:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor`
4. Doppelklicken Sie im Detailfenster auf "Start".
5. Geben Sie im Feld "Wert" den Wert "4" ein, klicken Sie auf Hexadezimal (sofern diese Option nicht bereits ausgewählt ist), und klicken Sie anschließend auf OK.
6. Beenden Sie den Registrierungs-Editor.

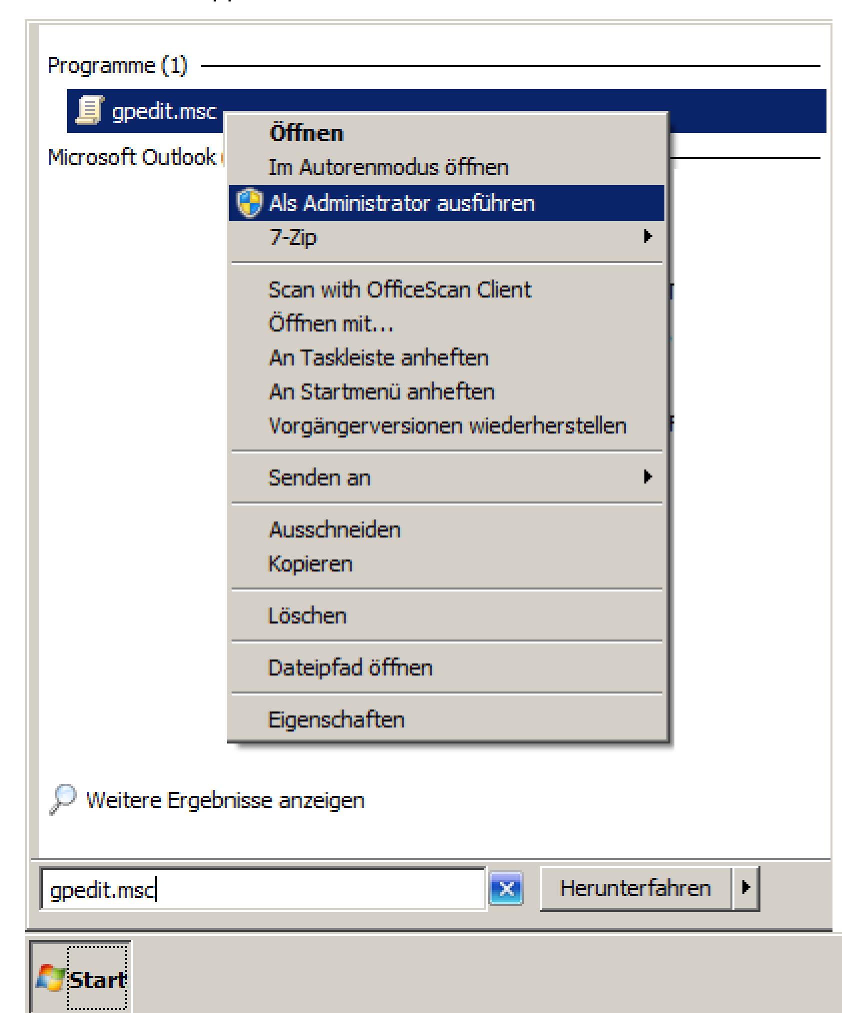
4.6.3 Sperren des Zugriffs auf USB-Speichermedien mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008

Vorgehensweise

1. Klicken Sie auf "Start" und geben Sie in das Feld "Suche" die Zeichenfolge "gpedit.msc" ein.



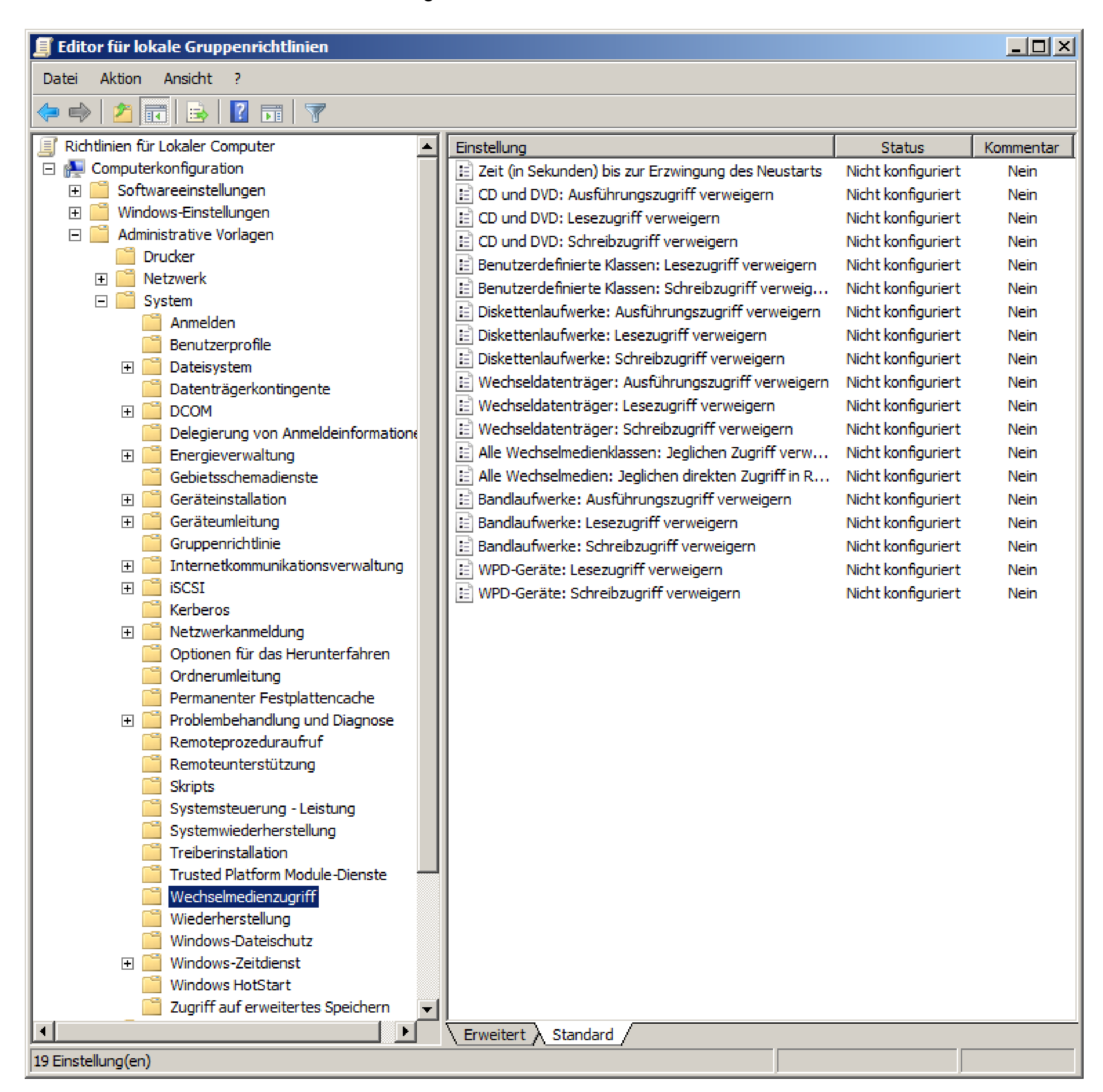
2. Starten des Gruppenrichtlinieneditor als Administrator.



Für diese Aktion sind Administratorenrechte notwendig. Melden Sie sich deshalb als Administrator an oder starten Sie den Gruppenrichtlinieneditor als Administrator. Geben Sie das Administratorpasswort ein, wenn dies erforderlich ist.

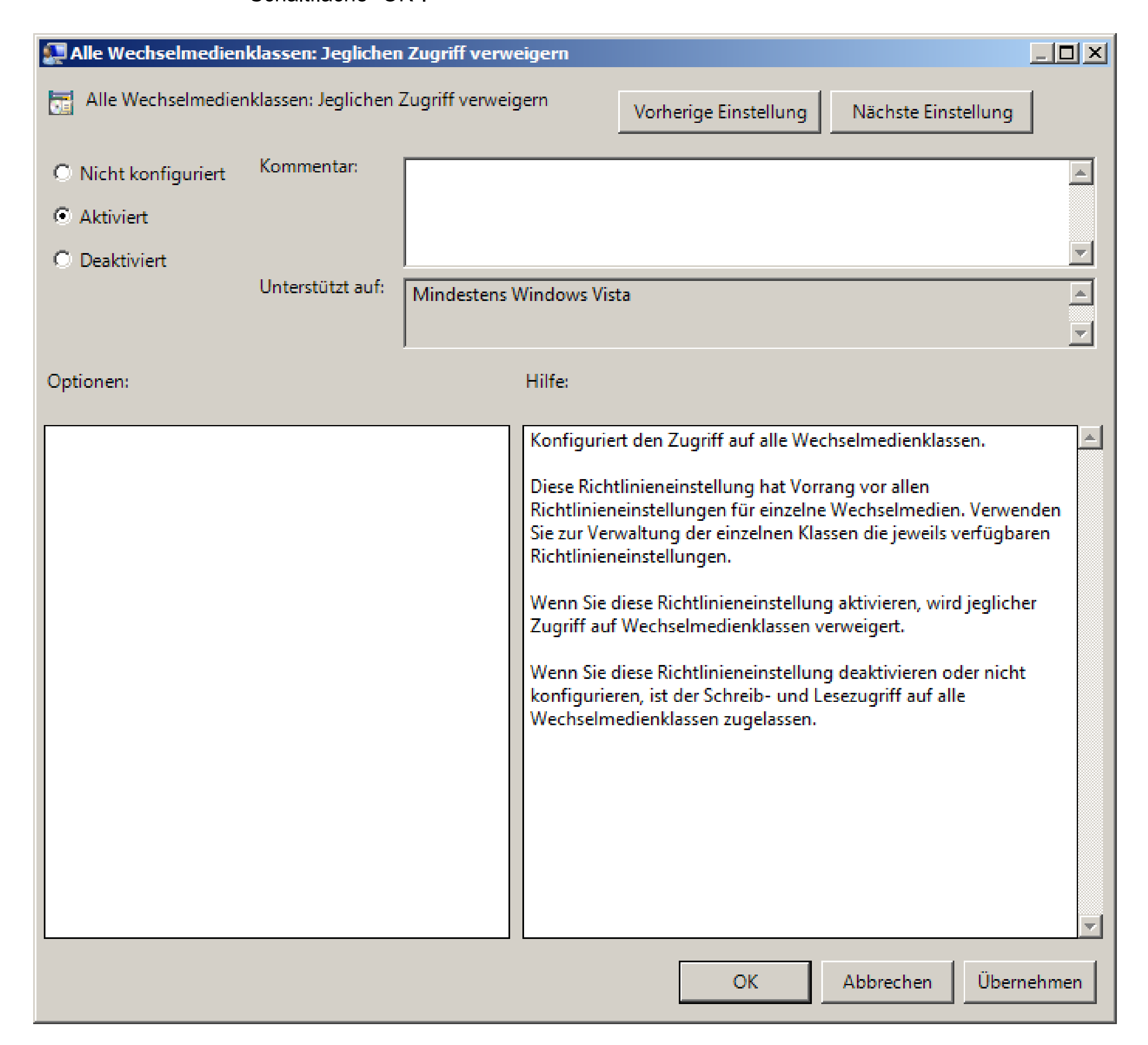
Der Gruppenrichtlinieneditor wird geöffnet.

3. Selektieren Sie den Ordner "Computerkonfiguration > Administrative Vorlagen > System > Wechselmedienzugriff".



4. Doppelklicken Sie die Gruppenrichtlinie "Alle Wechselmedienklassen: Jeglichen Zugriff verweigern".
   Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.

5. Wählen Sie die Option "Aktiviert" und bestätigen Sie die Einstellungen mit der Schaltfläche "OK".



6. Starten Sie anschließend den Rechner neu.

Hinweis

Der Zugriff auf USB-Speichermedien kann auch mithilfe einer globalen Gruppenrichtlinie in einer Domain zentral für alle Rechner gesperrt werden.

4.6.4 Reglementierung der Nutzung von auf USB-Speichermedien mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008

Um ein USB Speichermedium auf einem Rechner zu verwenden, muss das Gerät installiert werden. Dies erfolgt grundsätzlich automatisch, wenn das Gerät das erste Mal mit einem Rechner verbunden wird. Diese Installation kann über Gruppenrichtlinien beeinflusst werden:

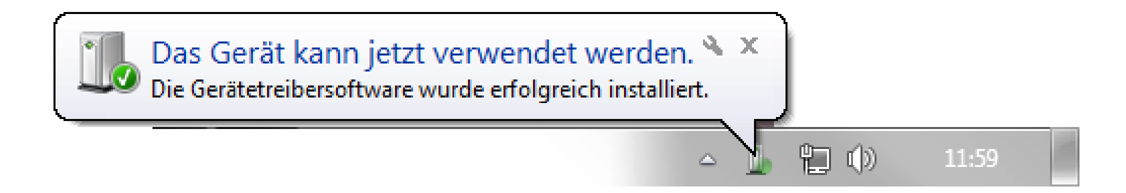
- Die Installation von explizit festgelegten Geräten durch den Anwender kann erlaubt werden (Positivliste)
- Die Installation von explizit festgelegten Geräten durch den Anwender kann unterbunden werden (Negativliste)
- Der Schreib- und Lesezugriff auf mobile Datenträger wie z.B. USB-Sticks, USB-HDDs, Disketten, CD-/DVD-Brenner kann konfiguriert werden.

Um die Installation eines Gerätes entsprechend den o.g. Fällen durch Gruppenrichtlinien zu beeinflussen, ist die Kenntnis der Hardware-ID des Gerätes notwendig.

Hardware-ID eines Gerätes zu ermitteln

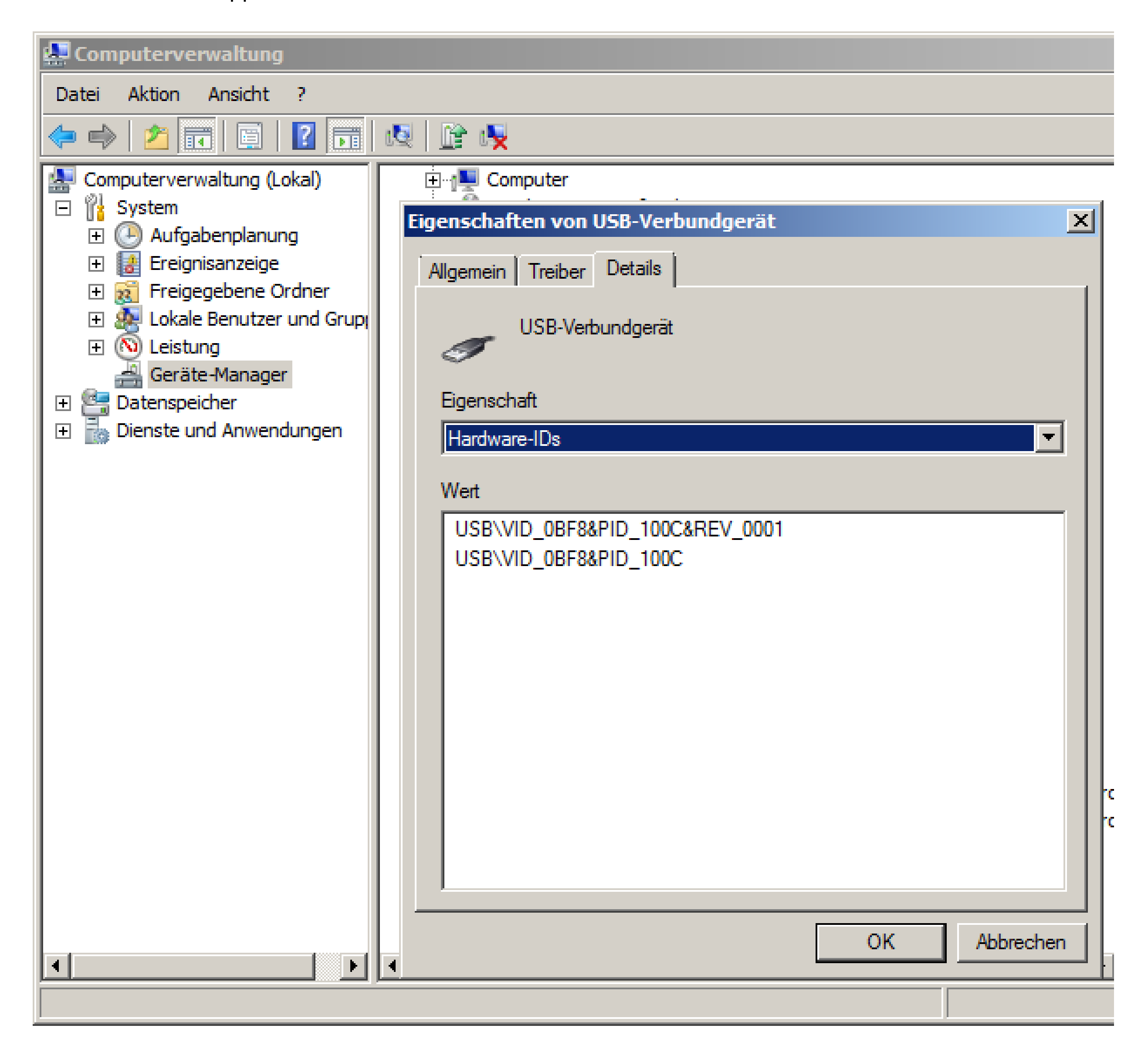
Um die Hardware-ID eines Gerätes zu ermitteln, gehen Sie folgendermaßen vor:

1. Verbinden Sie das Gerät mit einem Windows-PC und warten Sie die Installation des entsprechenden Treibers ab.
   Die erfolgreiche Installation wird durch die Meldung "Das Gerät kann jetzt verwendet werden" angezeigt.



2. Öffnen Sie nach erfolgreicher Gerätetreiberinstallation den Gerätemanager.
3. Öffnen Sie den Eigenschaftsdialog des entsprechenden Gerätes und klicken Sie auf die Registerkarte "Details".

4. Wählen Sie den Eintrag "Hardware-IDs" aus der Klappliste, um die Hardware-IDs des Geräts anzuzeigen.
   Die Hardware-IDs benötigen Sie zur Konfiguration der entsprechenden Gruppenrichtlinien.



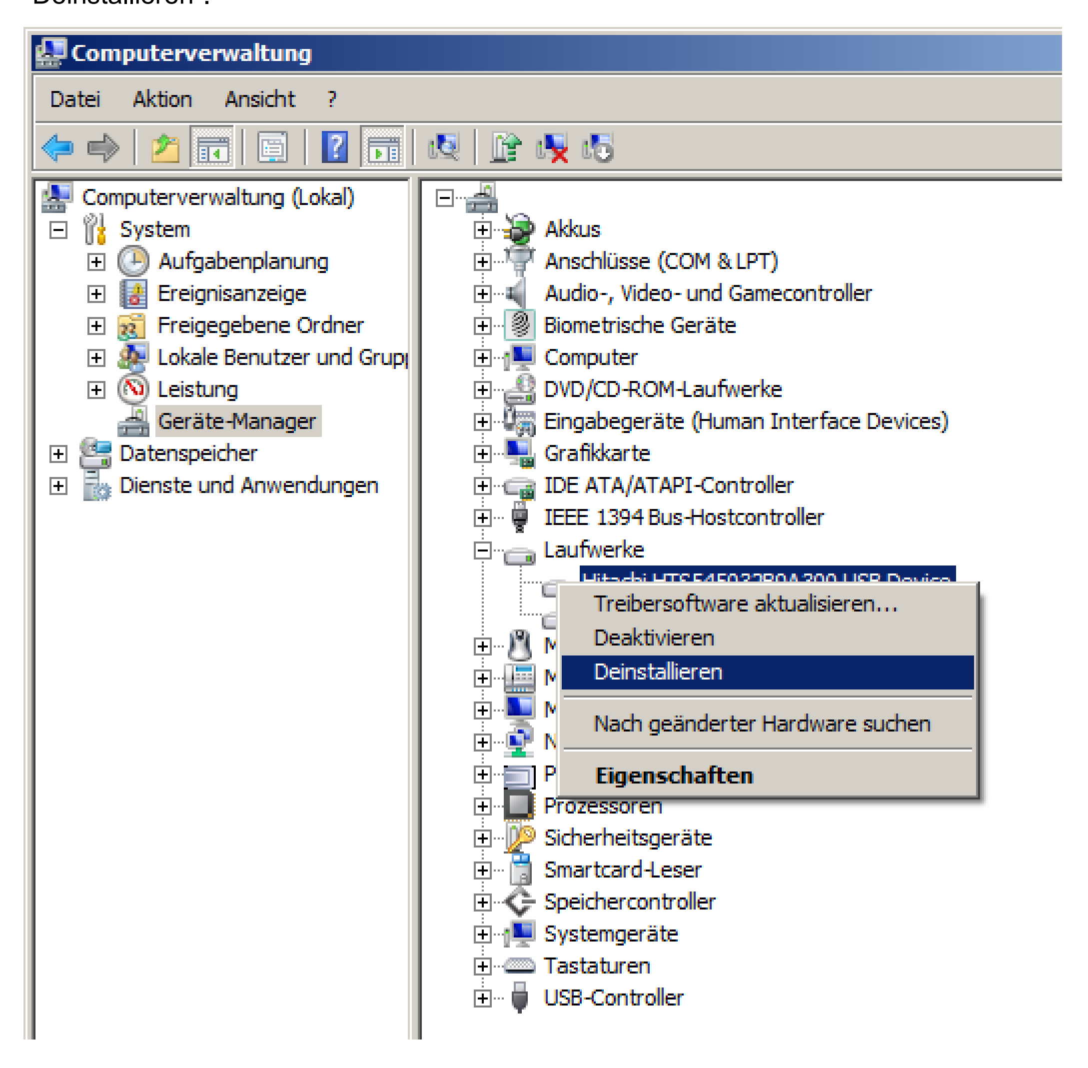
5. Wählen Sie den Eintrag "Kompatible IDs" aus der Klappliste aus, um die kompatiblen IDs des Geräts anzuzeigen.
   Die kompatiblen IDs benötigen Sie zur Konfiguration der entsprechenden Gruppenrichtlinien.

Gerät deinstallieren

Nach der Ermittlung der Hardware-ID muss das Gerät deinstalliert werden. In einem folgenden Schritt geben Sie die Installation des Geräts über Gruppenlichtlinien explizit frei.

Um das Gerät zu deinstallieren, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie den Befehl "Deinstallieren".



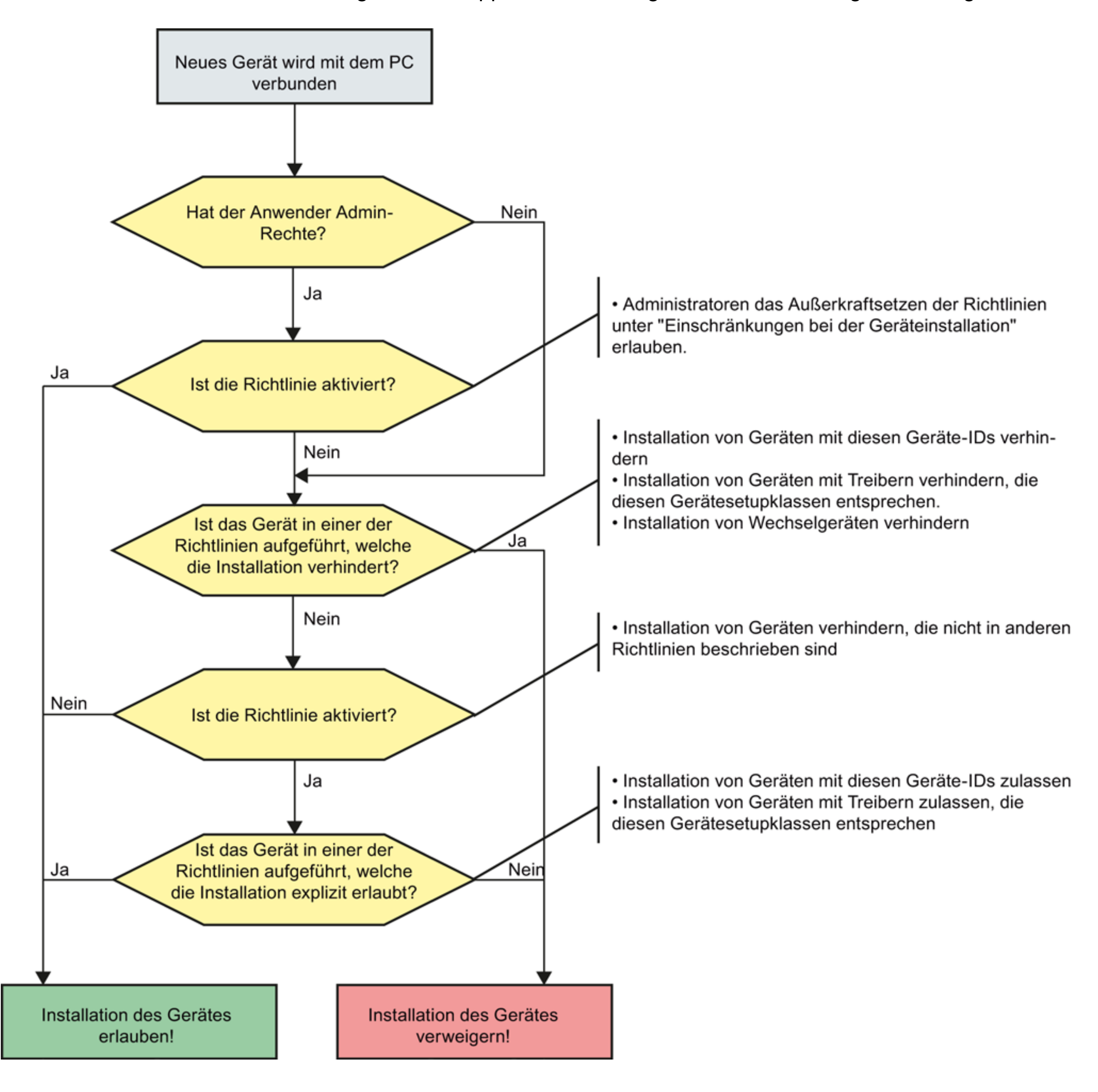
2. Klicken Sie im abschließenden Dialog auf die Schaltfläche "OK".

Zusammenhang der Gruppenrichtlinien

Das Verhalten der Geräteinstallation kann durch Gruppenrichtlinien bestimmt werden. Diese Gruppenrichtlinien finden Sie im Gruppenrichtlinieneditor unter "Computerkonfiguration > Administrative Vorlagen > System >Geräteinstallation> Einschränkungen bei der Geräteinstallation". Dort finden Sie die folgenden Richtlinien:

- Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben
- Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind
- Installation von Geräten mit diesen Geräte-IDs zulassen
- Installation von Geräten mit diesen Geräte-IDs verhindern.
- Installation von Geräten mit Treibern zulassen, die diesen Geräte-Setup-Klassen entsprechen
- Installation von Geräten mit Treibern verhindern, die diesen Geräte-Setup-Klassen entsprechen
- Installation von Wechselgeräten verhindern

Der Zusammenhang dieser Gruppenrichtlinien ergibt sich aus dem folgenden Diagramm:



Wenn Sie unter Beachtung der o.g. Gruppenrichtlinien an einem Rechner nur ganz bestimmte Geräte zulassen möchten, gehen Sie folgendermaßen vor:

1. Verhindern Sie die die Installation aller Geräte auf dem Rechner.
2. Geben Sie explizit ein bestimmtes Gerät zur Installation frei.

Um die Installation aller Geräte auf dem Rechner zu verhindern, gehen Sie folgendermaßen vor:

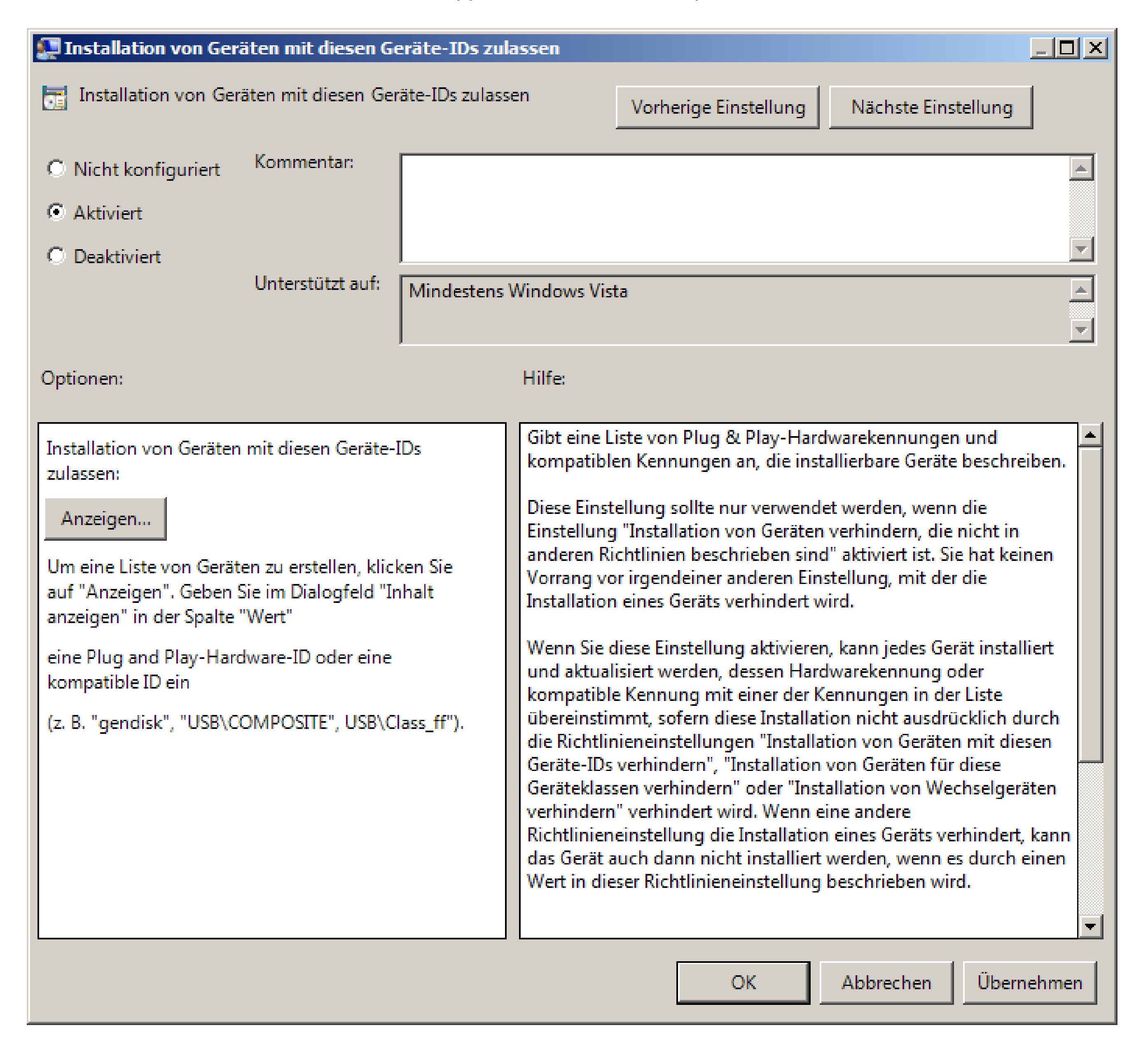
1. Stellen Sie sicher, dass alle Geräte im Gerätemanager deinstalliert sind.
2. Starten Sie den Gruppenrichtlinieneditor und navigieren Sie zum Ordner "Computerkonfiguration > Administrative Vorlagen > System >Geräteinstallation> Einschränkungen bei der Geräteinstallation".
   Die Gruppenrichtlinien werden im rechten Bereich des Editors angezeigt.
3. Öffnen Sie die Eigenschaften der Gruppenrichtlinie "Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind" durch Doppelklick auf die Richtlinie.
   Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.
4. Aktivieren Sie die Gruppenrichtlinie über die Option "Aktiviert" und bestätigen Sie die Einstellung mit der Schaltfläche "OK".
   Die Installation aller Geräte auf dem Rechner ist unterbunden.

Im nächsten Schritt stellen Sie ein, dass für Benutzer mit Administratorenrechten das Außerkraftsetzen der Richtlinien unter "Einhaltung bei der Geräteinstallation" erlaubt ist. Somit können Administratoren auf dem Rechner mit aktivierter, eingeschränkter Geräteinstallation über den Assistenten zum Hinzufügen von Hardware-Treiber installieren. Um diese Gruppenrichtlinie zu aktivieren, gehen Sie folgendermaßen vor:

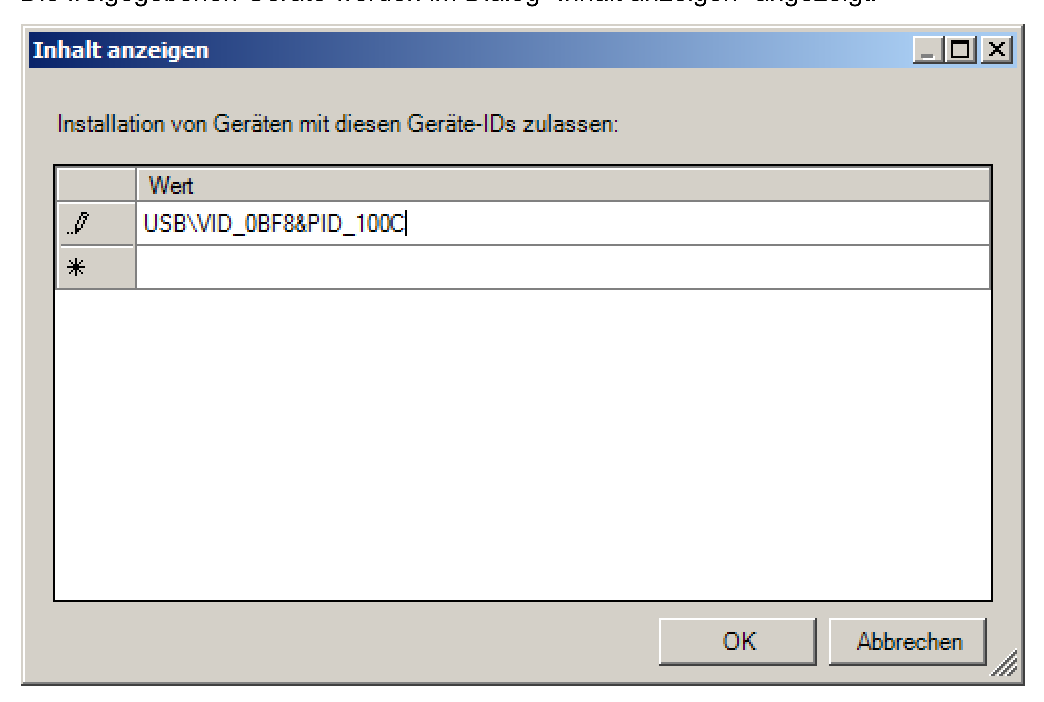
1. Öffnen Sie die Eigenschaften der Gruppenrichtlinie "Administratoren das Außerkraftsetzen der Richtlinien unter 'Einschränkungen bei der Geräteinstallation' erlauben" durch Doppelklick auf die Richtlinie.
   Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.
2. Aktivieren Sie die Gruppenrichtlinie über die Option "Aktiviert" und bestätigen Sie die Einstellung mit der Schaltfläche "OK".

Im nächsten Schritt geben Sie bestimmte Geräte zur Installation frei (Positivliste). Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Eigenschaften der Gruppenrichtlinie "Installation von Geräten mit diesen Geräte-IDs zulassen" durch Doppelklick auf die Richtlinie.
   Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.
2. Aktivieren Sie die Gruppenrichtlinie über die Option "Aktiviert".



3. Klicken Sie auf die Schaltfläche "Anzeigen", um die Geräte anzuzeigen, die auf Ihrem Rechner zur Installation freigegeben sind.
   Die freigegebenen Geräte werden im Dialog "Inhalt anzeigen" angezeigt.



4. Um weitere Geräte zur Installation auf Ihrem Rechner freizugeben, geben Sie die Hardware-IDs der Geräte in den Dialog ein.
   Die Hardware-IDs der Geräte können Sie mithilfe des Geräte-Managers ermitteln.
5. Bestätigen Sie die Einstellungen mit der Schaltfläche "OK".
   Auf Ihrem Rechner sind die Installation und die Verwendung der eingegebenen Geräte durch die Benutzer erlaubt. Der Administrator unterliegt nicht dieser Einschränkung.

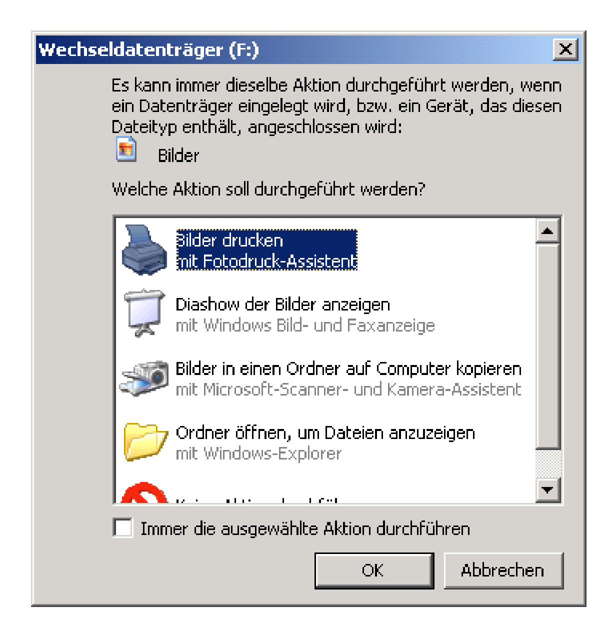
4.6.5 Windows AutoRun / AutoPlay für CD/DVD-Laufwerke und USB-Speichermedien deaktivieren

Quelle: http://support.microsoft.com/kb/967715/de

Die Hauptaufgabe von Autorun besteht darin, auf Hardwareaktionen, die auf einem Rechner gestartet werden, softwareseitig zu reagieren. Autorun bietet die folgenden Funktionen:

- Doppelklicken
- Kontextmenü
- Automatische Wiedergabe

Diese Funktionen werden typischerweise von Wechselmedien oder Netzwerkfreigaben aufgerufen. Während der automatischen Wiedergabe wird die Datei "Autorun.inf" auf dem Medium gesucht und, wenn vorhanden, analysiert. Diese Datei legt fest, welche Befehle vom System ausgeführt werden. Üblicherweise wird diese Funktionalität zum Starten von Installationsprogrammen genutzt. Aber über diese Funktion kann auch Schadsoftware wie z. B. Trojaner gestartet werden.



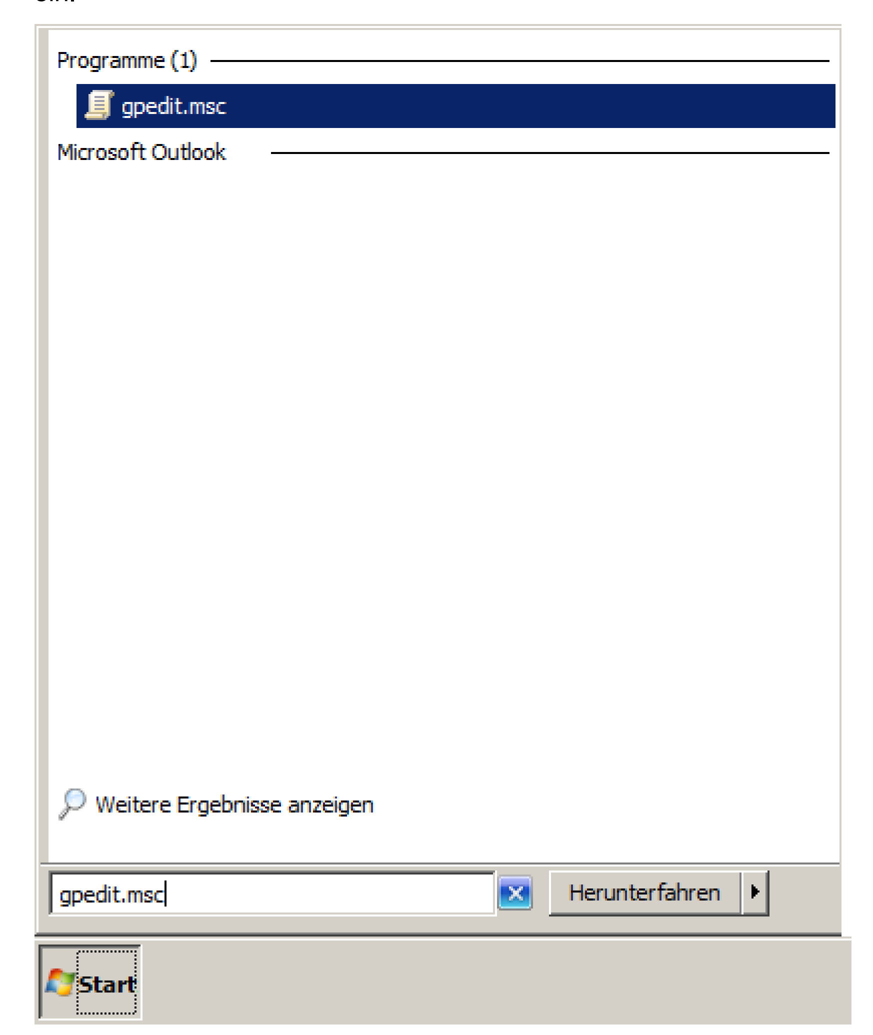
Verantwortlich für AutoRun und auch für AutoPlay ist der Dienst "Shellhardwareerkennung" (ShellHWDetection). Unter Windows XP kann der Dienst deaktiviert werden, wenn man AutoRun ohnehin deaktiviert hat.

4.6.5.1 Deaktivieren der AutoPlay-Funktion mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008

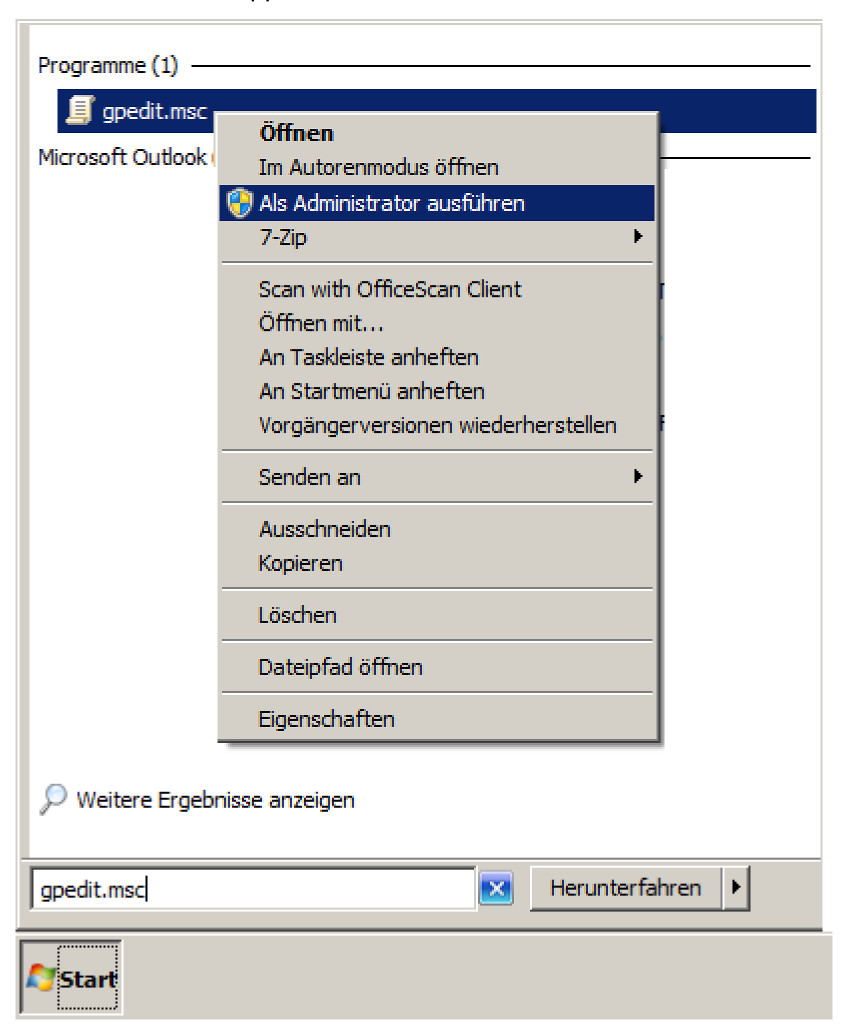
Vorgehensweise

Um die AutoPlay-Funktion zu deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf "Start" und geben Sie in das Feld "Suche" die Zeichenfolge "gpedit.msc" ein.



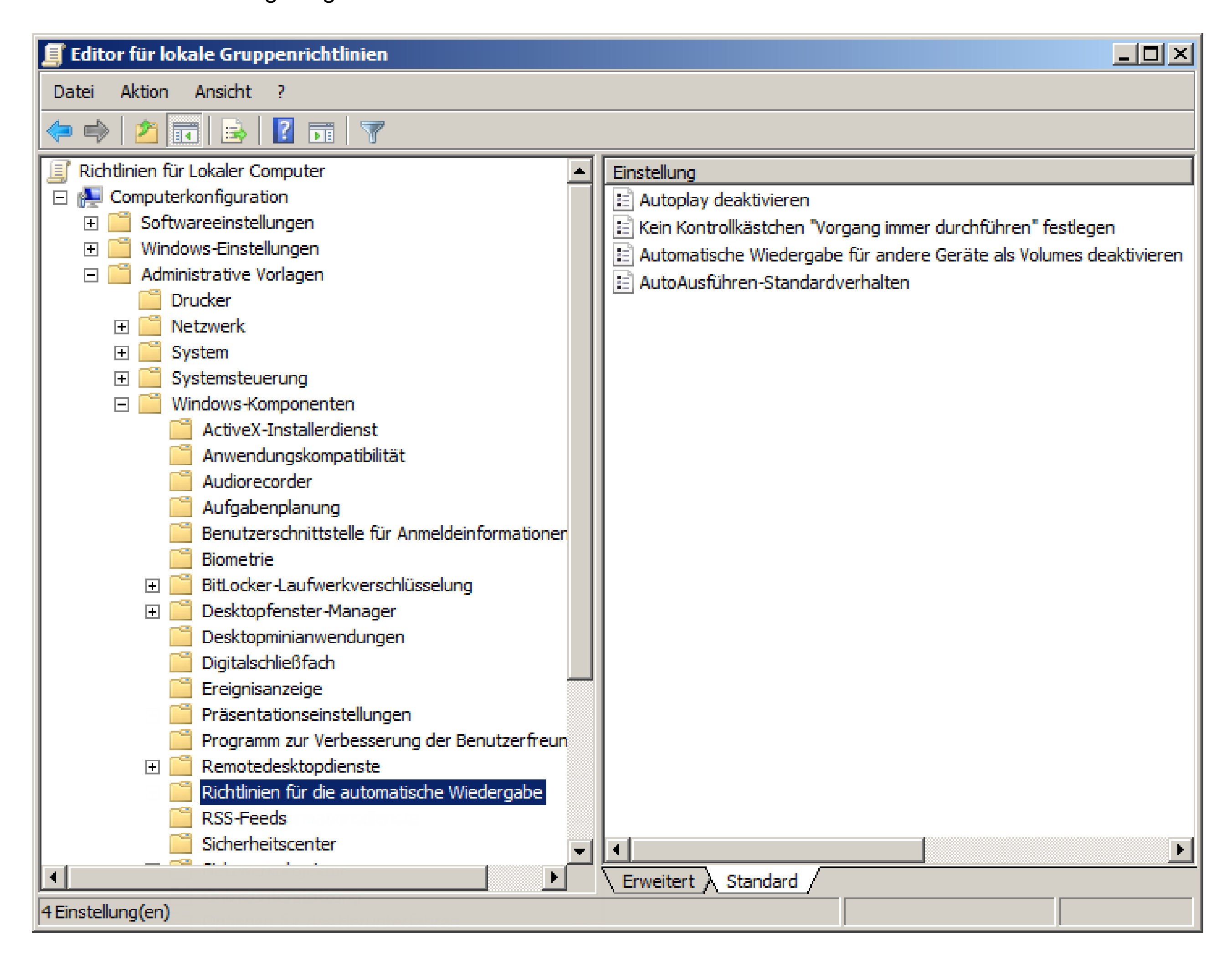
2. Starten Sie den Gruppenrichtlinieneditor als Administrator.



Für diese Aktion sind Administratorenrechte notwendig. Melden Sie sich deshalb als Administrator an oder starten Sie den Gruppenrichtlinieneditor als Administrator. Geben Sie das Administratorenpasswort ein, wenn dies erforderlich ist.
Der Gruppenrichtlinieneditor wird geöffnet.

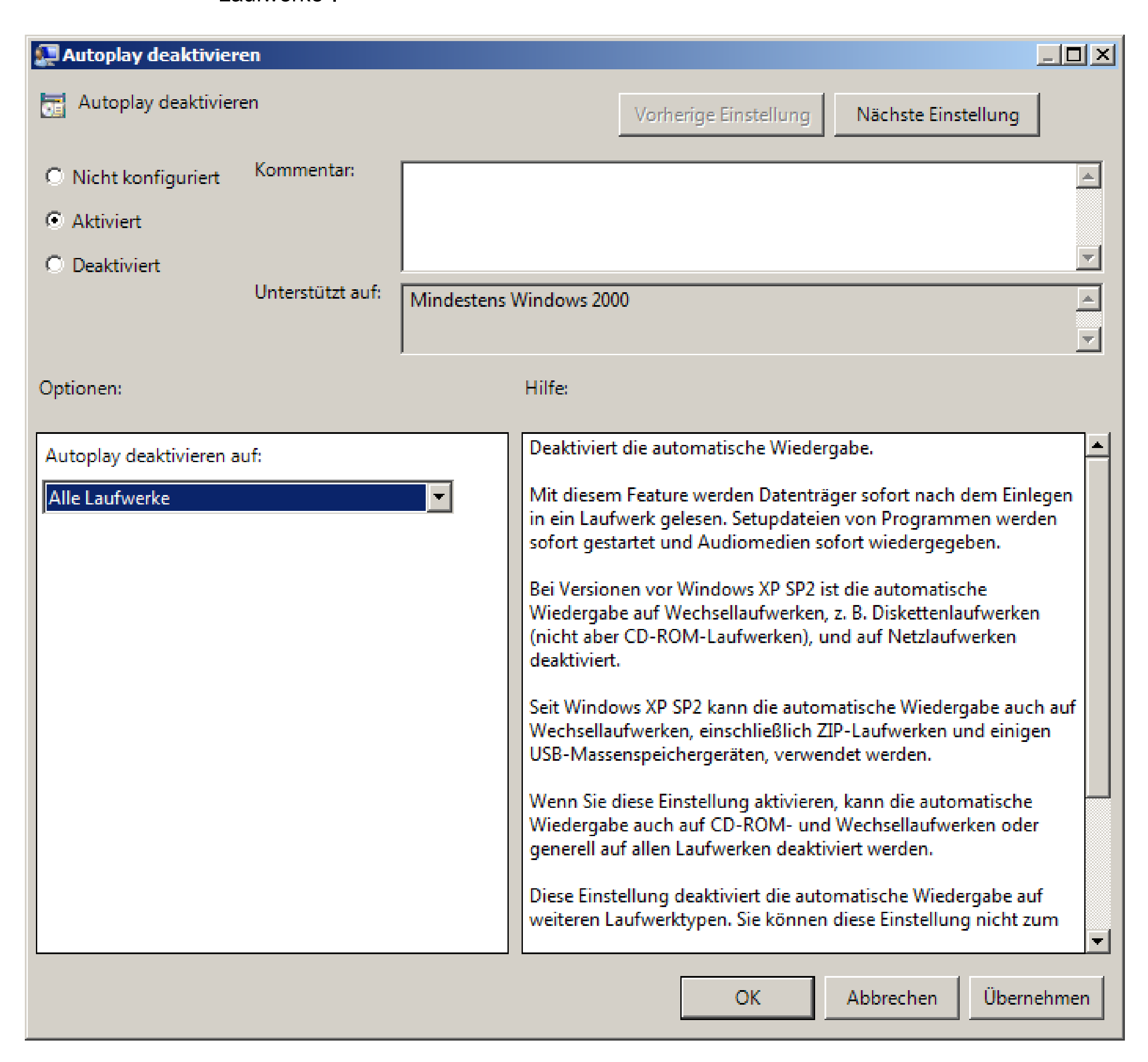
3. Selektieren Sie den Ordner "Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Richtlinien für die automatische Wiedergabe".

   Im rechten Bereich des Editors werden die zum Ordner zugehörigen Richtlinien angezeigt.



4. Doppelklicken Sie die Gruppenrichtlinie "Autoplay deaktivieren".
   Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.
5. Wählen Sie die Option "Aktiviert".

6. Wählen Sie aus der Klappliste im Bereich "Autoplay deaktivieren auf:" die Option "Alle Laufwerke".



7. Bestätigen Sie die Einstellungen mit der Schaltfläche "OK".
8. Starten Sie anschließend den Rechner neu.

4.6.5.2 Deaktivieren der AutoPlay-Funktion mittels Gruppenrichtlinie in Windows XP und Windows Server 2003

Vorgehensweise

Um die AutoPlay-Funktion zu deaktivieren, gehen Sie folgendermaßen vor:

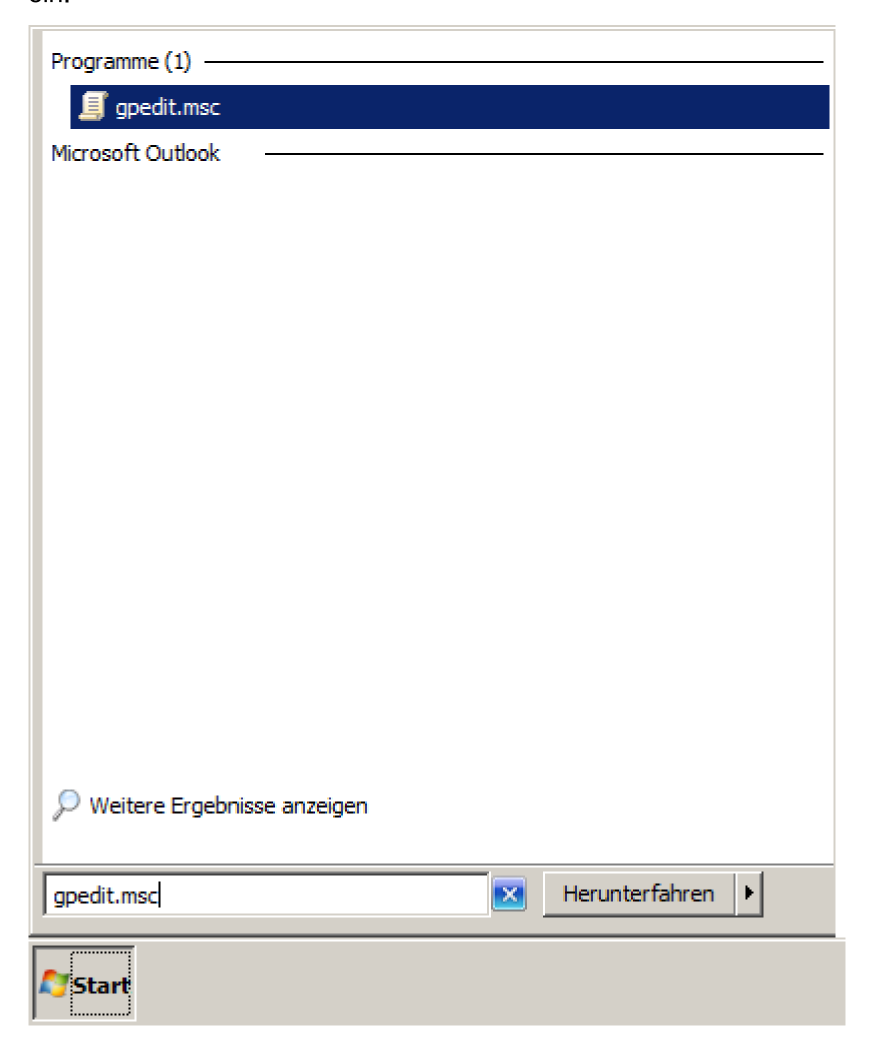
1. Klicken Sie auf "Start" und dann auf "Ausführen".
2. Geben Sie in das Feld "Öffnen" die Zeichenfolge "gpedit.msc" ein und klicken Sie auf die Schaltfläche "OK".
   Der Gruppenrichtlinieneditor wird geöffnet.
3. Selektieren Sie den Ordner "Computerkonfiguration > Administrative Vorlagen > System".
   Im rechten Bereich des Editors werden die zum Ordner zugehörigen Richtlinien angezeigt.
4. Doppelklicken Sie die Gruppenrichtlinie "Autoplay deaktivieren".
   Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.
5. Wählen Sie die Option "Aktiviert".
6. Wählen Sie aus der Klappliste im Bereich "Autoplay deaktivieren auf:" die Option "Alle Laufwerke".
7. Bestätigen Sie die Einstellungen mit der Schaltfläche "OK".
8. Starten Sie anschließend den Rechner neu.

4.6.5.3 Deaktivieren aller AutoRun-Funktionen mittels Gruppenrichtlinie in Windows 7 und Windows Server 2008

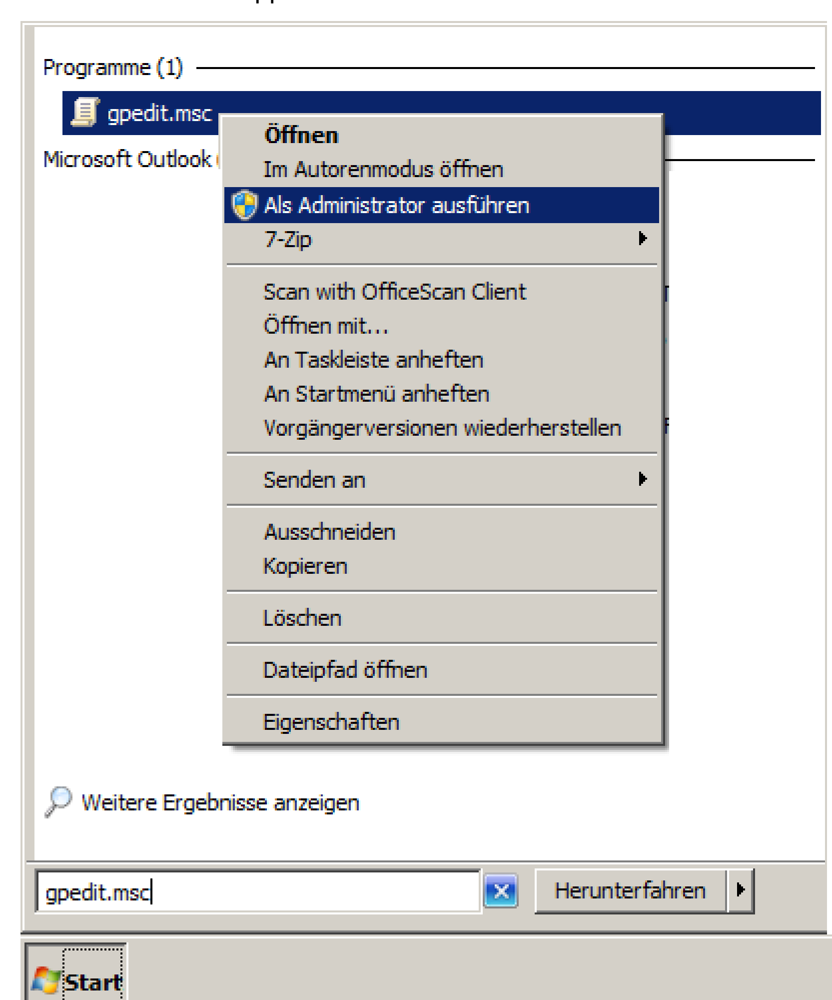
Vorgehensweise

Um die AutoRun-Funktion zu deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf "Start" und geben Sie in das Feld "Suche" die Zeichenfolge "gpedit.msc" ein.



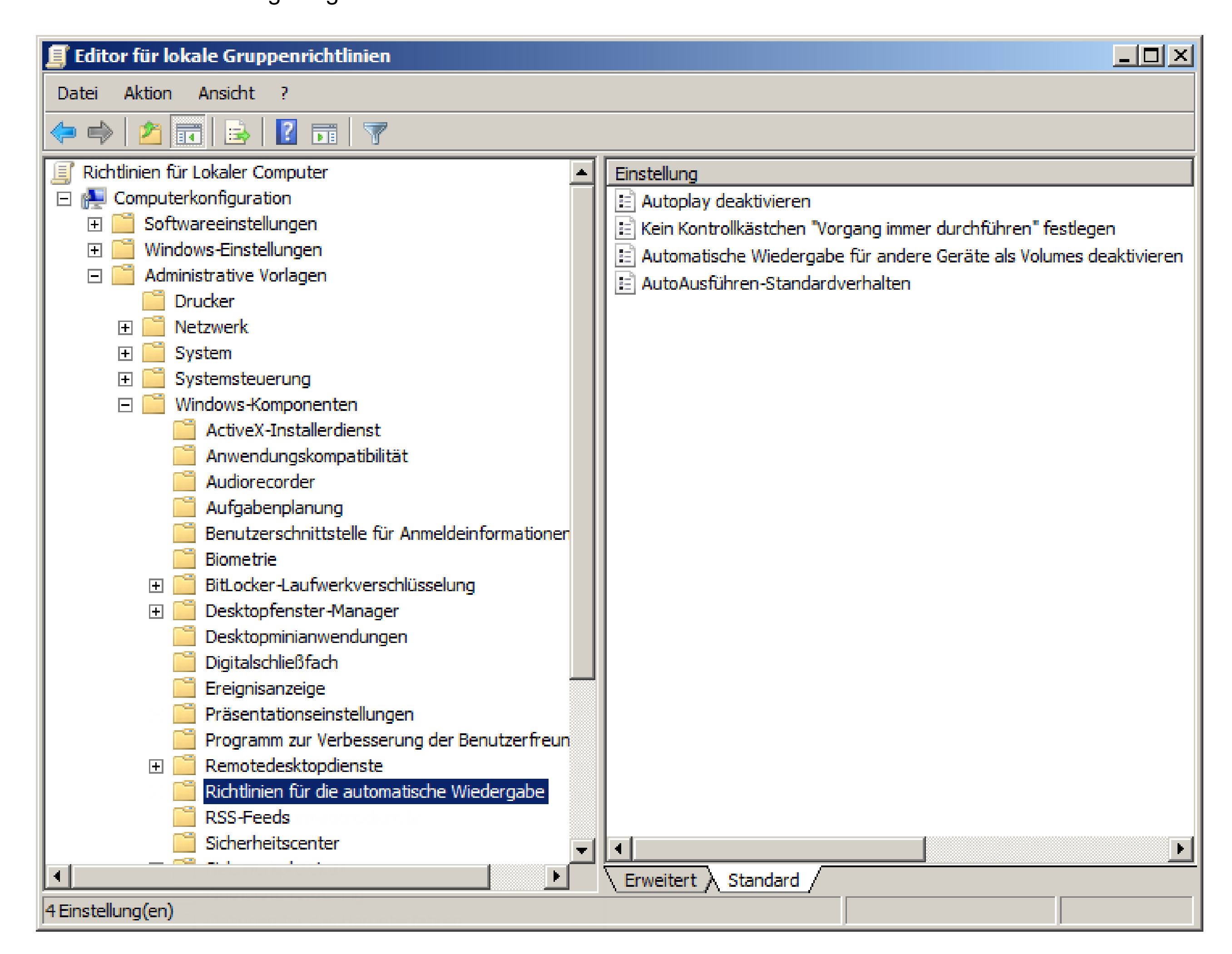
2. Starten Sie den Gruppenrichtlinieneditor als Administrator.



Für diese Aktion sind Administratorenrechte notwendig. Melden Sie sich deshalb als Administrator an oder starten Sie den Gruppenrichtlinieneditor als Administrator. Geben Sie das Administratorenpasswort ein, wenn dies erforderlich ist. Der Gruppenrichtlinieneditor wird geöffnet.

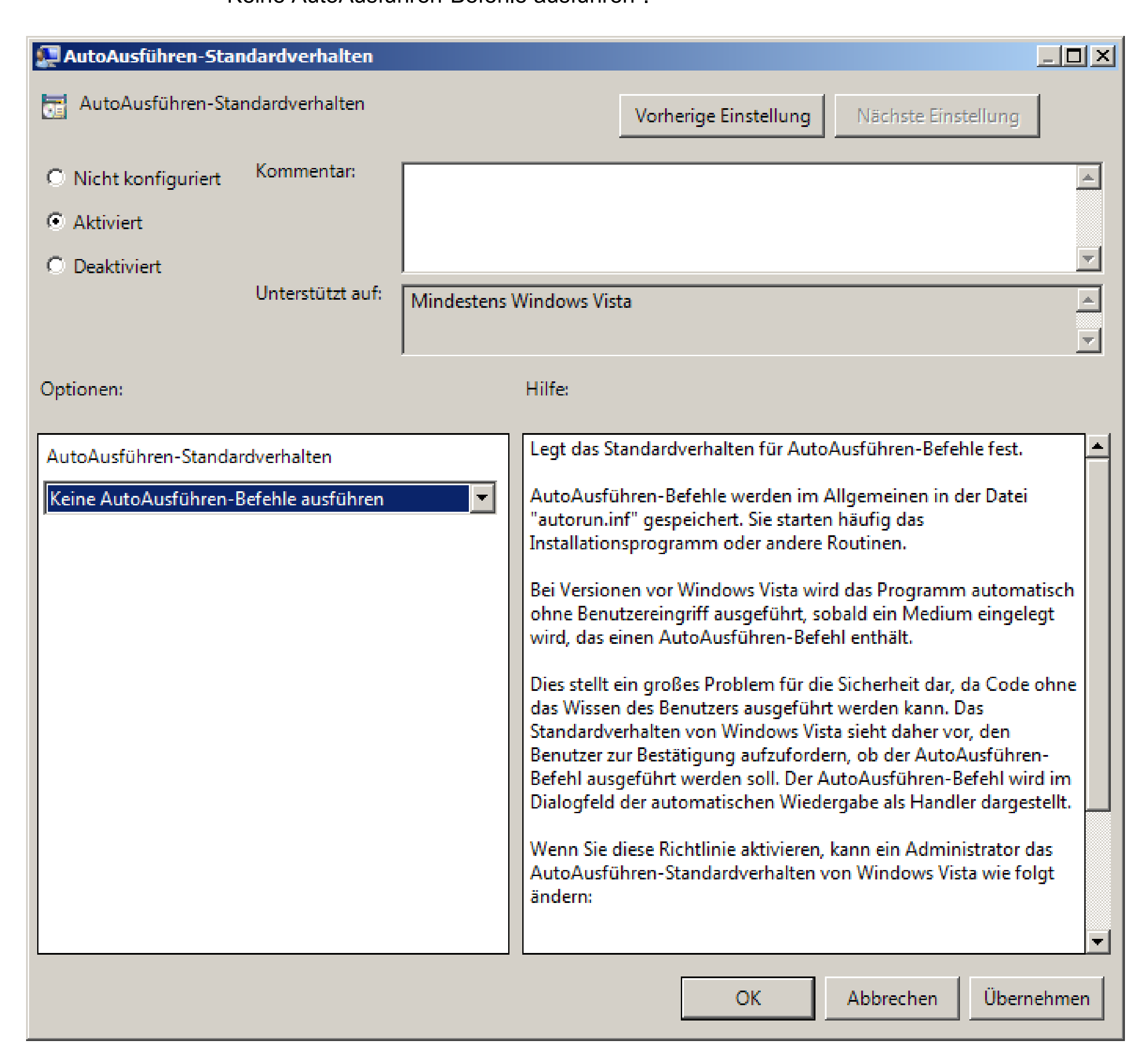
3. Selektieren Sie den Ordner "Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Richtlinien für die automatische Wiedergabe".

   Im rechten Bereich des Editors werden die zum Ordner zugehörigen Richtlinien angezeigt.



4. Doppelklicken Sie die Gruppenrichtlinie "AutoAusführen-Standardverhalten". Der Eigenschaftsdialog der Gruppenrichtlinie wird geöffnet.
5. Wählen Sie die Option "Aktiviert".

6. Wählen Sie aus der Klappliste im Bereich "AutoAusführen-Standardverhalten" die Option "Keine AutoAusführen-Befehle ausführen".



7. Bestätigen Sie die Einstellungen mit der Schaltfläche "OK".
8. Starten Sie anschließend den Rechner neu.

4.7 Whitelisting

Einleitung

Der Ansatz des Whitelisting besteht darin, dass auf dem Rechnersystem nur Anwendungen ausgeführt werden, die als vertrauenswürdig gelten. Diese Anwendungen werden in einer Positivliste (Whitelist) gepflegt. Aufgrund der Positivliste ist bei Withelisting ein ständiges Anpassen an neue Bedrohungen in Form von Schadsoftware nicht notwendig.

McAfee Application Control

Mit McAfee Application Control können nicht autorisierte Anwendungen auf Servern und Workstations blockiert werden. Dies bedeutet, dass nach der Installation und Aktivierung von McAfee Application Control auf einem Rechnersystem, alle ausführbaren Dateien vor Veränderung geschützt sind und verhindert wird, dass unbekannte (nicht auf der Whitelist vorhandene) ausführbare Dateien gestartet werden können.

Im Vergleich zu einfachen Whitelisting-Konzepten verwendet McAfee Application Control ein dynamisches Vertrauenswürdigkeitsmodell. Damit sind keine langwierigen manuellen Aktualisierungen von Listen genehmigter Anwendungen notwendig. Aktualisierungen können auf unterschiedliche Weise eingebracht werden:

- Durch vertrauenswürdige Benutzer (Benutzer)
- Durch vertrauenswürdige Hersteller (Zertifikat)
- Von einem vertrauenswürdigen Verzeichnis
- Durch Binärdatei
- Mittels Updater (Aktualisierungsprogramme z.B. WSUS, Virenscanner)

Des Weiteren bietet McAfee Application Control eine Funktion, die den Speicher überwacht, vor einem Pufferüberlauf (Buffer Overflow) schützt und Dateien im Speicher absichert.

Die Verwaltung bzw. Administration von McAfee Application Control kann auf folgende Weise erfolgen:

- Lokal auf einem Rechnersystem (Standalone)
- Zentral über McAfee ePolicy Orchestrator (ePO)

Die Entscheidung, ob die Verwaltung von McAfee Application Control lokal oder zentral erfolgt, soll aufgrund der Anzahl der zu pflegenden Systeme getroffen werden.

Unabhängig von der Art der Verwaltung gilt die folgende Vorgehensweise:

- Nach der Installation von McAfee Application Control auf einem Rechner muss zuerst ein "solidify" des Rechners ausgeführt werden. Dies bedeutet, dass alle angeschlossenen lokalen Laufwerke nach ausführbaren Dateien durchsucht werden. Die Dauer dieser Prozedur ist abhängig von der Datenmenge und der Rechnerleistung und kann mehrere Stunden dauern. Bei aktueller Hardware mit PCS 7 OS-Server-Installation und mittelgroßen Projekten dauert dies beispielsweise ca. 20-30 Minuten.
- Nachdem McAfee Application Control aktiviert wurde, muss ein Neustart des Rechners durchgeführt werden. Alle während der Prüfung gefundenen, ausführbaren Dateien (exe, com, dll, bat, usw.) werden nun vor Änderungen (Umbenennung, Löschung, usw.) geschützt. Es können keine neuen Dateien ausgeführt werden.

Lokale Verwaltung von McAfee Application Control

Die lokale Verwaltung erfolgt ausschließlich über die Kommandozeile. Die Befehle sind verständlich und selbsterklärend. Des Weiteren bietet McAfee gute Dokumentationen an. McAfee Application Control kann gut über bat-Dateien oder Skripte gesteuert werden.

Zentrale Verwaltung von McAfee Application Control mittels McAfee ePO

McAfee ePO soll auf einem eigenen Rechner mit aktueller Hardware installiert werden. Gibt es in der Anlage bereits einen Infrastruktur-Rechner (z.B. WSUS, Virenscan-Server) kann McAfee ePO auch auf diesem installiert werden. McAfee ePO darf nicht auf einem Automatisierungsgerät oder einem Domain-Controller installiert werden.

Die zentrale Verwaltung (Installation, Konfiguration und Überwachung) erfolgt über McAfee ePO (McAfee ePolicy Orchestrator). McAfee ePO ist ein Management Tool, das alle McAfee Produkte verwalten kann und viele zum Teil kostenlose Netzwerkmanagement- und Netzwerküberwachungsfunktionalitäten mit sich bringt.

Ähnlich wie bei einer Active Directory-Domain gilt auch hier, dass ab ca. 10 verwalteten Systemen eine zentrale Verwaltung genutzt werden soll. Alle lokalen McAfee Application Control-Befehle und -Optionen sind auch remote über die ePO verfügbar und zum Teil über vordefinierte Tasks, der Rest über remote Kommandozeilen-Optionen. Die ePO bietet, im Vergleich zur lokalen Verwaltung, eine bessere Überwachung und ein übersichtlicheres Eventmanagement.

Weitere Informationen

Die Whitelist-Lösung von McAfee Application Control ist für verschiedene SIMATIC PCS 7-Versionen freigegeben. Details über die Kompatibilität zu SIMATIC PCS 7 finden Sie unter http://support.automation.siemens.com/WW/view/de/2334224.

Eine Beschreibung der empfohlenen Vorgehensweise mit McAfee Application Control finden Sie unter http://support.automation.siemens.com/WW/view/de/51776157.

Zusätzlich zu den bereits beschriebenen Systemhärtungsmöglichkeiten gibt es weitere Möglichkeiten, die auch Themen wie z. B. Device-Härtung (von Netzwerkgeräten und PLC´s) miteinbeziehen. Diese sind in den Industrial Security Services enthalten. Weitere Informationen und die entsprechenden Ansprechpartner finden Sie unter http://www.industry.siemens.com/topics/global/de/industrial-security/seiten/default.aspx.

Sie können Ihre Anfrage per E-Mail auch direkt an "industrialsecurity.i@siemens.com" richten.

4.8 SIMATIC S7 CPUs

Seitdem die S7-400 Steuerung die kritischste Komponente in einer PCS 7 Konfiguration ist, wird empfohlen, ein Passwort und eine geeignete Schutzstufe zu vergeben. Das Passwort sollte eine ausreichende Komplexität haben. Das bedeutet z. B., dass das Passwort aus Buchstaben, Sonderzeichen und Zahlen besteht und eine Länge von mindestens 8 Zeichen hat.

Für S7-400 CPUs kann im Projekt eine Schutzstufe definiert werden, um einen nicht autorisierten Zugriff auf das CPU Programm zu verhindern.

Es kann zwischen drei Schutzstufen gewählt werden. Dabei hat die Schutzstufe 1 keine Zugriffsrestriktion und die Schutzstufe 3 die strengste Zugriffrestriktion.

Es wird empfohlen mindestens die Schutzstufe 2 zu konfigurieren.

Detaillierte Information zu den Schutzstufen von S7-400 CPUs finden Sie unter http://support.automation.siemens.com/WW/view/de/60458386.

Wenn S7-400 CPUs mit integriertem Web Server (S7-400 PN Standard) eingesetzt werden, muss darauf geachtet werden, dass der Web Server in der CPU deaktiviert ist.

Benutzerverwaltung und Bedienberechtigungen 5

5.1 Übersicht

Unter der Verwaltung von Benutzer- und Bedienberechtigungen werden die Vergabe der Berechtigungen in der Windows-Umgebung und die Zuordnung der Benutzer zu tätigkeitsorientierten Rollen verstanden. Diese Verfahren sind konsequent voneinander getrennt, werden aber beide streng unter dem Prinzip der minimal benötigten Rechte angewandt. Eine einfache Überprüfung kann mit den folgenden Fragen durchgeführt werden:

- Wer muss was können?
- Wer darf was?

Beim Anmelden am Betriebssystem muss der Benutzer die Rechte erhalten, die für die Bewältigung seiner Aufgaben erforderlich sind.

Beim Anmelden am Leitsystem (z. B. an der Bedienstation OS-Client oder am Engineering System usw.) muss der Bediener/Engineer die Berechtigungen erhalten, die er in seiner Rolle (z. B. als Bediener einer Teilanlage) benötigt.

5.2 Windows-Arbeitsgruppe oder Windows-Domain

Bei der Verwendung einer Windows-Arbeitsgruppe ist die Verwaltung der Computer und Benutzer dezentralisiert und lokal auf jedem einzelnen Computer. Innerhalb einer Windows-Domain (Active Directory) ist eine zentrale Verwaltung von Computern und Benutzern möglich.

Wann sollen Anlagen in einer Windows-Arbeitsgruppe betrieben werden?

Der Betrieb einer Anlage ohne zentrale Windows-Verwaltung wird unter folgenden Bedingungen empfohlen:

- Die Anlage hat nicht mehr als ca. 10 Computer.
- In der Anlage werden keine regelmäßigen Änderungen vorgenommen (z. B. Hinzufügen neuer Benutzer, Austausch von Computern, Einführung neuer Sicherheitsrichtlinien, Passwortänderungen, usw.).
- Der Betrieb einer Windows-Domain-Infrastruktur kann aufgrund des fehlenden Fachpersonals nicht gewährleistet werden.
- Die Einheitlichkeit von Netzwerkeinstellungen, Computerkonfigurationen, Sicherheitsrichtlinien, Benutzern und Passwörtern kann durch eine zentrale Anlagendokumentation gewährleistet werden.

Folgendes soll beachtet werden:

- Passwörter von Benutzern müssen bei allen betroffenen Computern geändert werden.
- Nicht mehr benötigte Benutzerkonten müssen überall entfernt werden.
- Auf allen Computern der Anlage müssen dieselben Sicherheitsrichtlinien konfiguriert werden (z. B. Verwendung des LanManager V2 Protokoll, Signierung der SMB-Kommunikation, Passwortkomplexität und Passwortalter).
- Eine zentrale Aufzeichnung von vergebenen Computernamen und IP-Adressen muss erstellt und aktuell gehalten werden.
- Wenn lokale LMHost- und Host-Dateien zur Namensauflösung genutzt werden, müssen diese Dateien immer zeitgleich aktualisiert werden.
- Der Betrieb einer kompletten Anlage kann durch die fehlerhafte Konfiguration eines einzelnen Computers gefährdet werden. Zudem ist die Fehlersuche in solchen Fällen oft schwierig und zeitaufwändig.

Wann sollen Anlagen in einer Windows-Domain (Active Directory) verwaltet werden?

Die Konfiguration einer zentralen Windows-Verwaltung wird unter folgenden Bedingungen empfohlen:

- Die Anlage hat mehr als 10 Computer oder die Anzahl der zu verwaltenden Computer, Konten und Benutzer sehr groß ist.
- In der Anlage werden regelmäßige Änderungen vorgenommen (z. B. Hinzufügen von Benutzern, Austausch von Computern, Einführung neuer Sicherheitsrichtlinien, Passwortänderungen, usw.).
- Ein fehlertolerantes Anmelden und eine fehlertolerante Benutzerverwaltung sind gefordert.
- Eine zentrale Konfiguration der Computer ist gefordert.
- Das Unternehmen hat eigene Sicherheitsrichtlinien, die eine Active Directory Domain erfordern.

Zusätzliche Kriterien für eine zentrale Verwaltung sind:

- Gesetzliche Anforderungen und Richtlinien müssen erfüllt werden (z. B. Nutzung von Kerberos als Authentifizierungsmethode oder zentrales Aufzeichnen von Anmeldeereignissen, usw.).
- Zentrale fehlertolerante IP-Adressenzuweisung (DHCP), zentrale Verwaltung der Namensauflösung und Registrierung der Computer (DNS/WINS) sind gefordert.

Hinweis

Ein fehlertoleranter DHCP ist erst mit einem DHCP-Server auf der Basis von Windows Server 2008 (oder neuer) möglich.

- Es bestehen folgende Anforderungen eines Zertifikatservers basierend auf Active Directory für Dienste:
  - Sichere Web Services mit verschlüsselter Kommunikation über Secure Socket Layer (SSL)
  - Signaturen für Anwendungen und Dokumente
  - Authentifizierung
  - Zertifikatsbasierende IP-Sicherheitskommunikationsprotokolle und Tunneling-Protokolle wie das Layer Two Tunneling Protocol (L2TP).

5.3 Verwaltung von Computern und Benutzern

Die Strategie der aufgabenbezogenen Bedienungs- und Zugriffsrechte (role-based access control) beinhaltet die Einschränkung auf minimal benötigte Rechte und Funktionen der Benutzer, Bediener, Geräte, Netzwerk- und Softwarekomponenten.

Die Benutzer, die in der Betriebssystemumgebung anzulegen sind, können dezentral oder zentral verwaltet werden.

Dabei ist Folgendes zu beachten:

- Bei der dezentralen Verwaltung der Benutzer in Arbeitsgruppen ist nach dem von Microsoft empfohlenen ALP-Prinzip (Add User Account to Local Group and assign Permission) vorzugehen. Dies bedeutet, dass lokale Benutzer zunächst gruppiert werden, um dann an diese Gruppen die notwendigen Berechtigungen (Ordner, Freigaben, etc.) zu vergeben.
- Wird die Verwaltung zentral mittels einer Domain durchgeführt, so ist die AGLP-Prinzip (Access-Global-Local-Permission) zu beachten. Nach diesem Prinzip werden die Benutzerkonten zunächst im Active Directory den Domain-globalen Gruppen zugeordnet. Diese Gruppen werden dann rechnerlokalen Gruppen zugeteilt, denen wiederum die Rechte an den Objekten vergeben werden.

Umsetzung

Bei einem Automatisierungssystem gibt es Stationen/Rechner die permanent in Betrieb sein müssen und von mehreren Personen genutzt werden. Ein Beispiel hierfür ist eine Bedien- und Beobachtungsstation (OS-Client). Diese Station wird permanent von unterschiedlichen Bedienern zur Prozessführung verwendet.

Es empfiehlt sich, für die Benutzerkonten dieser permanent verwendeten Bedien- und Beobachtungsstationen "nicht-personifizierte", gerätespezifische Benutzerkonten zu verwenden. Hier bieten sich Konten an, die einen Bezug zu dem jeweiligen Rechner herstellen lassen (z.B. OSClient_5). Bei der Verwendung von "Autologon" zur Anmeldung am Betriebssystem muss dieses Konto verwendet werden. Für eine Engineering Station, die nicht permanent in Betrieb ist, aber von unterschiedlichen Benutzern/Engineer zum Projektieren verwendet wird, bieten sich personenbezogene Benutzerkonten pro Benutzer/Engineer an.

Hinweis

Die Mitgliedschaft in der Administratorengruppe ist nur für die Installation von PCS 7 und die Konfiguration des Rechners relevant.

SIMATIC-Berechtigungsmodell

Alle Rechte an Freigaben und Ordnern, die im Zusammenhang mit SIMATIC-Produkten stehen, können über das SIMATIC-Berechtigungsmodell vergeben werden. Dazu werden bereits während der Installation lokale Gruppen angelegt, die dann samt den benötigten Berechtigungen den SIMATIC-Objekten hinzugefügt werden. Dies vereinfacht die Erteilung der Sicherheitseinstellungen, da das jeweilige Benutzerkonto bzw. die Gruppe nur der lokalen SIMATIC-Gruppe hinzugefügt werden muss. In Abhängigkeit davon, welche SIMATIC-Produkte installiert werden, kann sich die Anzahl der hinzugefügten Gruppen unterscheiden.

Neben den von SIMATIC angelegten Gruppen ist auch die Mitgliedschaft in der lokalen Standardgruppe "Benutzer" erforderlich. Die Mitgliedschaft in der Benutzergruppe "SIMATIC HMI" ermöglicht zwar den Zugriff auf die Projekte, erteilt jedoch nicht die Berechtigung auf das Betriebssystem zuzugreifen oder sich lokal am Desktop anzumelden.

SIMATIC WinCC

Bei der Installation von SIMATIC WinCC werden die folgenden drei neuen Benutzergruppen angelegt, die für die Projektfreigaben und die Projektdateizugriffe verwendet werden:

- SIMATIC HMI
  Die Mitglieder dieser Gruppe dürfen lokal Projekte anlegen, bearbeiten, starten und auf diese Projekte remote zugreifen. Standardmäßig werden der Benutzer, der die Installation ausführt und der lokale Administrator in diese Gruppe automatisch aufgenommen. Weitere Benutzer müssen manuell durch einen Administrator dieser Gruppe hinzugefügt werden.
- SIMATIC HMI CS
  Die Mitglieder dieser Gruppe dürfen nur projektieren, jedoch keine Änderungen an den Laufzeitkomponenten direkt durchführen. Diese Gruppe ist standardmäßig leer und wird zur späteren Verwendung reserviert.
- SIMATIC HMI VIEWER
  Die Mitglieder dieser Gruppe dürfen nur lesend auf die Projektierung und Laufzeitdaten zugreifen. Diese Gruppe wird vorrangig für die Konten von Web-Veröffentlichungsdiensten verwendet, z. B. den IIS (Internet Information Services), der für den Betrieb des WinCC Web Navigator verwendet wird.

Beim erstmaligen Öffnen eines Projekts wird automatisch eine Projektfreigabe angelegt und mit den notwendigen Freigabeberechtigungen und Sicherheitseinstellungen versehen. Die Verwaltung der Projektfreigaben und Projektdateizugriffe erfolgt automatisch durch die SIMATIC-Software.

SIMATIC NET

Bei der Installation von SIMATIC NET über das Rahmensetup von SIMATIC PCS 7 wird der Benutzer- und Gruppenverwaltung die folgende lokale Benutzergruppe hinzugefügt:

- SIMATIC NET
  Alle Benutzer, die mit PCS 7, PCS 7 OS oder Route Control Projekten arbeiten, müssen Mitglied dieser Gruppe sein.

SIMATIC BATCH

Für SIMATIC BATCH wird bei der Installation folgende neue Benutzergruppe angelegt:

- SIMATIC BATCH
  Die Mitglieder dieser Gruppe haben vollen Zugriff auf die SIMATIC BATCH-Verzeichnisse "sbdata" und "sbdata_backup". Alle Benutzerkonten, die mit SIMATIC BATCH arbeiten, müssen Mitglied dieser Gruppe sein.

Die folgende Freigabe wird neu angelegt:

- BATCH

Die Verwaltung der Freigabeberechtigungen erfolgt bei der Installation. Fügen Sie in den Sicherheitseinstellungen der Freigaben zusätzlich die Benutzergruppe "SIMATIC BATCH" mit der Berechtigung Vollzugriff hinzu (NTFS-Berechtigungen). In diesen Freigaben werden später die Batch-Daten abgelegt.

SIMATIC Route Control

Für SIMATIC Route Control werden bei der Installation zusätzlich folgende Benutzergruppen angelegt:

- RC_ENGINEER
- RC_MAINTENANCE
- RC_OPERATOR_L1
- RC_OPERATOR_L2
- RC_OPERATOR_L3

Standardmäßig wird bei der Installation das installierende Benutzerkonto in die Gruppe "RC_MAINTENANCE" hinzugefügt.

Außerdem wird folgende Freigabe eingerichtet:

- RC_LOAD

Die Freigabeberechtigungen und Sicherheitseinstellungen erfolgen automatisch während der Installation. Die Einstellungen sind für alle fünf Gruppen einheitlich. Somit erfolgt der Zugriff auf das Projekt unabhängig davon, welcher Gruppe das angemeldete Konto zugeordnet wird. In diesen Freigaben werden später die RC-Daten abgelegt.

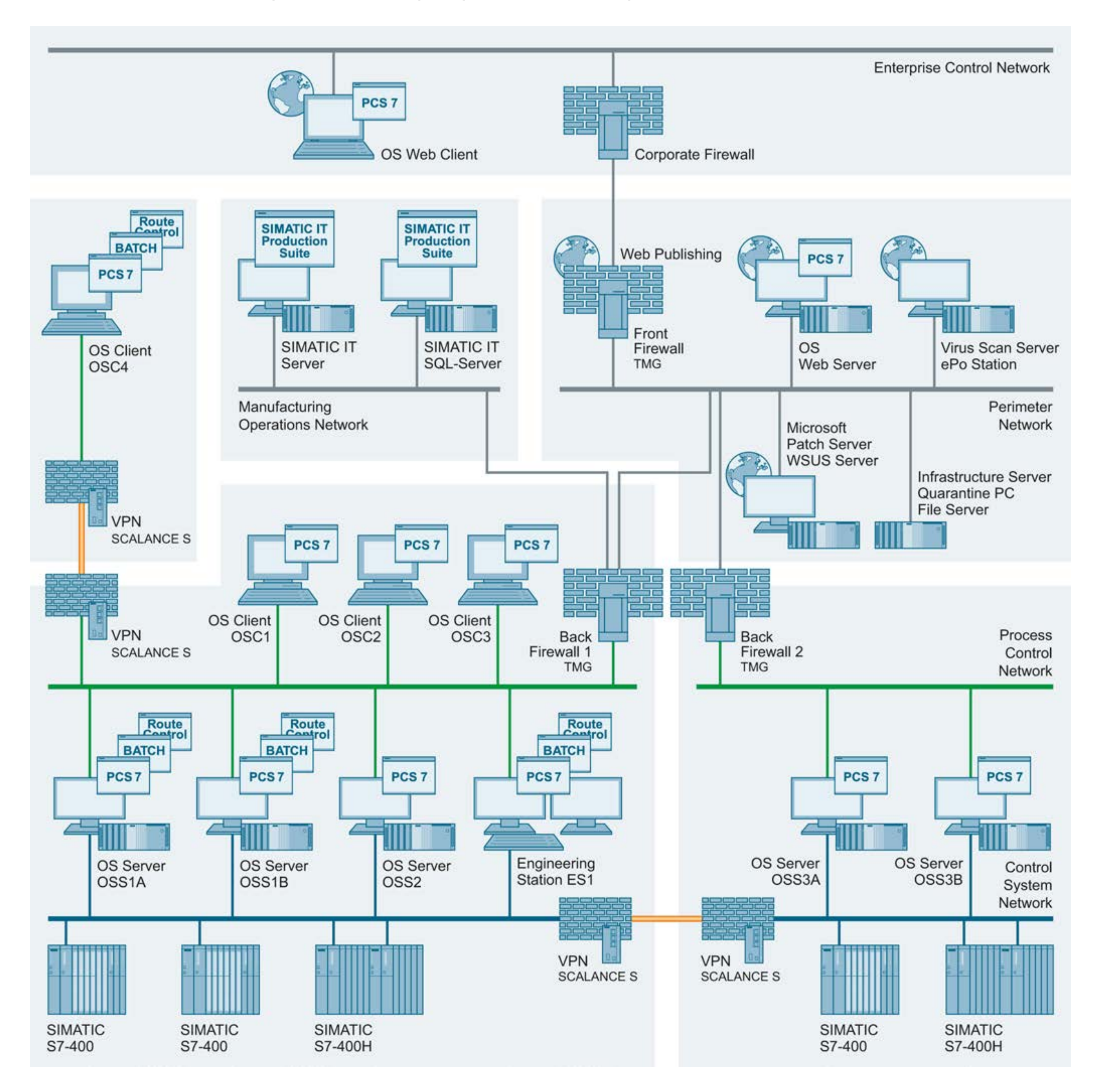
SIMATIC Management Console

Für die SIMATIC Management Console müssen die folgenden Benutzergruppen angelegt werden:

- SIMATIC Management Administrators
  Mitglieder dieser Gruppe erhalten uneingeschränkten Zugriff und alle Berechtigungen für die Management Console.
  Tragen Sie die Mitglieder dieser Gruppe an den Zielrechnern in die Gruppe der Administratoren ein. Damit sind die
  Mitglieder dieser Gruppe berechtigt, Änderungen der installierten Software auszuführen.
- SIMATIC Management Users
  Mitglieder dieser Gruppe erhalten einen eingeschränkten Zugriff und die Berechtigung "Nur Lesen" für die Management Console.
  Tragen Sie die Benutzer, die auf dem Rechner der Management Console der Benutzergruppe "SIMATIC Management Administrators" zugeordnet sind, auch in die Benutzergruppe "SIMATIC Management Users" ein.
- Windows-Anmeldung auf dem Rechner der Management Console
  Alle Benutzer der Management Console müssen sich als Administrator anmelden (lokale Gruppe "Administratoren" oder rechnerspezifischer Administrator in der Domain).

Musterkonfiguration

Die folgende Abbildung zeigt die Musterkonfiguration:



Für die Musterkonfiguration werden entsprechend den in diesem Kapitel aufgeführten Empfehlungen die folgenden Benutzer angelegt:

Benutzer	Beschreibung
ENG1	PCS 7-Projekteur 1 • Projektiert auf der Engineering Station (ES) mit SIMATIC Manager, HWKonfig, NetPro, CFC, SFC und WinCC • Lädt die Automatisierungssysteme und die OS-Server von der ES • Führt auch Bedienungen an den OS-Clients aus
ENG2	PCS 7-Projekteur 2 Zusätzlich zu ENG1 ist dieser Benutzer der Administrator der Anlage
OSC1	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Client "OSC1" angemeldet ist (gerätespezifisch, "nicht-personifiziert"). Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSC2	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Client "OSC2" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSC3	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Client "OSC3" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSC4	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Client OSC4 angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSS1A	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Server "OSS1A" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSS1B	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Server "OSS1B" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSS2	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Server "OSS2" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSS3A	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Server "OSS3A" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.
OSS3B	Lokaler Windows-Benutzer, der standardmäßig, permanent am OS-Server "OSS3B" angemeldet ist (gerätespezifisch, "nicht-personifiziert") Anmeldung am Betriebssystem erfolgt mittels Windows Autologon.

Die folgende Tabelle zeigt, welchen unterschiedlichen Benutzergruppen die o.g. Benutzer zugeordnet werden müssen:

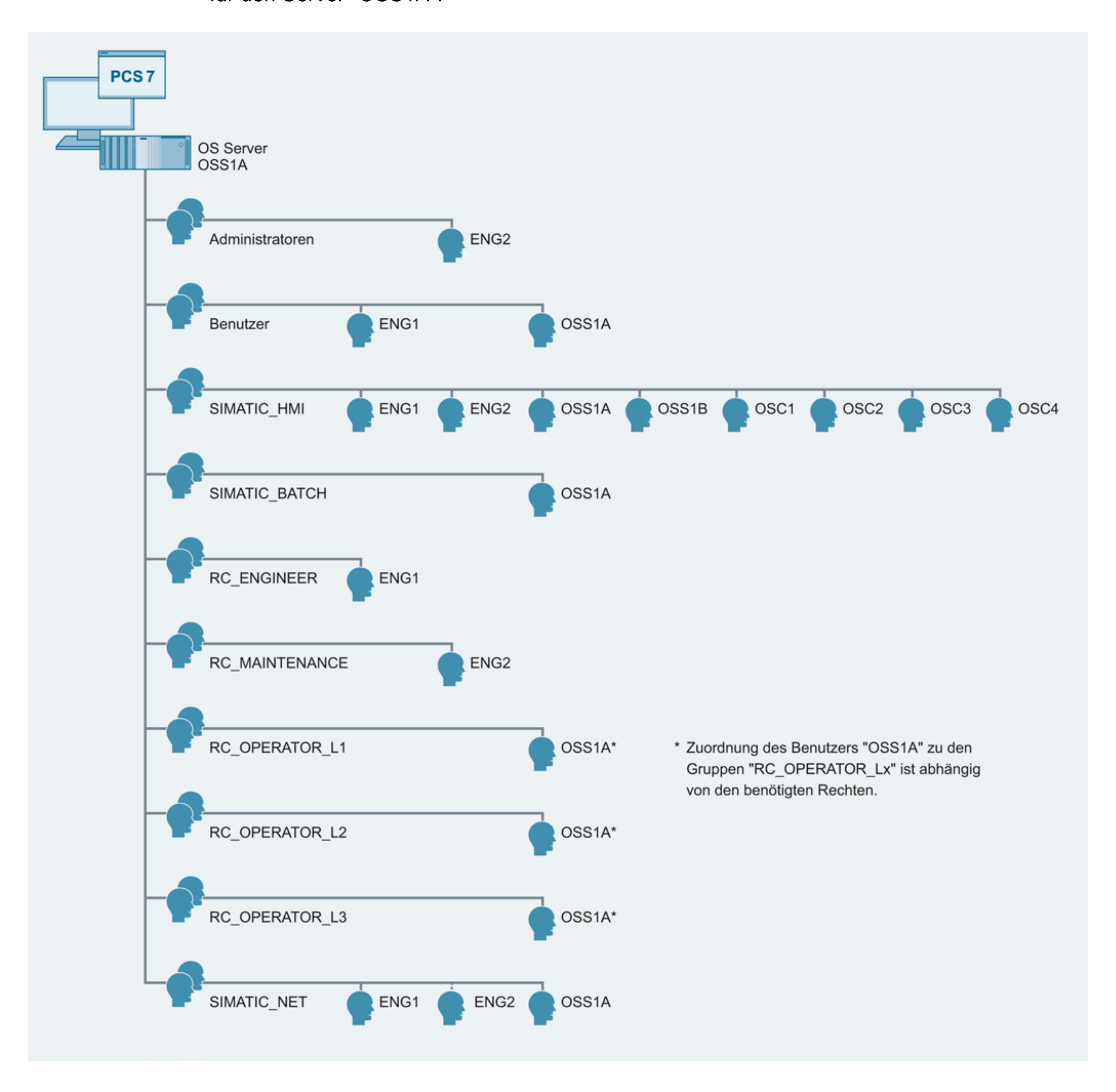
Rechner/ Lokale Gruppe	**ES1**	**OSC1**	**OSC2**	**OSC3**	**OSC4**	**OSS1A**	**OSS1B**	**OSS2**	**OSS3A**	**OSS3B**
Administratoren	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2	ENG2
Benutzer	ENG1	OSC1 ENG1	OSC2 ENG1	OSC3 ENG1	OSC4 ENG1	OSS1A ENG1	OSS1B ENG1	OSS2 ENG1	OSS3A ENG1	OSS3B ENG1
SIMATIC HMI	ENG1 ENG2	ENG1 ENG2 OSC1 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC2 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC3 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSC4 OSS1A OSS1B OSS2 OSS3A OSS3B	ENG1 ENG2 OSS1A OSS1B OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS1B OSS1A OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS2 OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS3A OSS3B OSC1 OSC2 OSC3 OSC4	ENG1 ENG2 OSS3B OSS3A OSC1 OSC2 OSC3 OSC4
SIMATIC BATCH[1)]	ENG1 ENG2	OSC1	OSC1	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A[1)]	OSS3B[1)]
RC_ENGINEERENG1[2)]	ENG1	-	-	-	-	ENG1	ENG1	ENG1	ENG1	ENG1
RC_MAINTENANCEENG1[2)]	ENG2	-	-	-	-	ENG2	ENG2	ENG2	ENG2	ENG2
RC_OPERATOR_L1[3)]	-	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
RC_OPERATOR_L2[3)]	-	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
RC_OPERATOR_L3[3)]	-	OSC1	OSC2	OSC3	OSC4	OSS1A	OSS1B	OSS2	OSS3A	OSS3B
SIMATIC NET	ENG1 ENG2	-	-	-	-	OSS1A ENG1 ENG2	OSS1B ENG1 ENG2	OSS2 ENG1 ENG2	OSS3A ENG1 ENG2	OSS3B ENG1 ENG2
Siemens TIA Engineer	ENG1 ENG2	-	-	-	-	-	-	-	-	-

[1)] Vorausgesetzt SIMATIC BATCH wird in der Musterkonfiguration benötigt/verwendet.

[2)] Vorausgesetzt SIMATIC Route Control wird in der Musterkonfiguration benötigt/verwendet.

[3)] Zuordnung des Benutzer OSC1 … 4 zu RC_OPERATOR_Lx ist abhängig von der notwendigen Berechtigung

Die folgende Abbildung zeigt beispielhaft die lokale Verwaltung der Benutzer und Gruppen für den Server "OSS1A":



Weitere Informationen

Weitere Informationen zur Rechner- und Benutzerverwaltung finden Sie im Dokument "Sicherheitskonzept PCS 7 und WinCC - Basisdokument (Whitepaper)" (http://support.automation.siemens.com/WW/view/de/26462131).

Beachten Sie zusätzlich die Informationen im Handbuch "SIMATIC Prozessleitsystem PCS 7 PC-Konfiguration und Autorisierung" (http://support.automation.siemens.com/WW/view/de/68157327).

Weitere Informationen zu Benutzerrechten bei SIMATIC Route Control, insbesondere in Bezug auf die Zuordnung der Benutzer zu den Benutzergruppen RC_OPERATOR_L1/L"/L3, finden Sie im Programmier- und Bedienhandbuch "SIMATIC Prozessleitsystem PCS 7 SIMATIC Route Control“ (http://support.automation.siemens.com/WW/view/de/68154021).

5.4 Passwortrichtlinien

Einleitung

Quelle: https://www.bsi.bund.de

Schlecht gewählte Passwörter sind nach wie vor eines der häufigsten Defizite bei der Sicherheit. Oft wählen die Nutzer zu kurze oder zu wenig komplexe Zeichenkombinationen.

Um Passwörter auszuspähen, nutzen Hacker zum Beispiel sogenannte Brute-Force-Angriffe, bei denen vollautomatisch eine Vielzahl möglicher Zeichenkombinationen ausprobiert oder ganze Wörterbücher getestet werden. Um solchen Angriffen vorzubeugen, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen.

Aus diesem Grund soll auf die Festlegung und die Umsetzung einer Passwortrichtlinie (Password Policy) in der Automatisierungsanlage geachtet werden. Eine solche Passwortrichtlinie sollte die folgenden Punkte berücksichtigen:

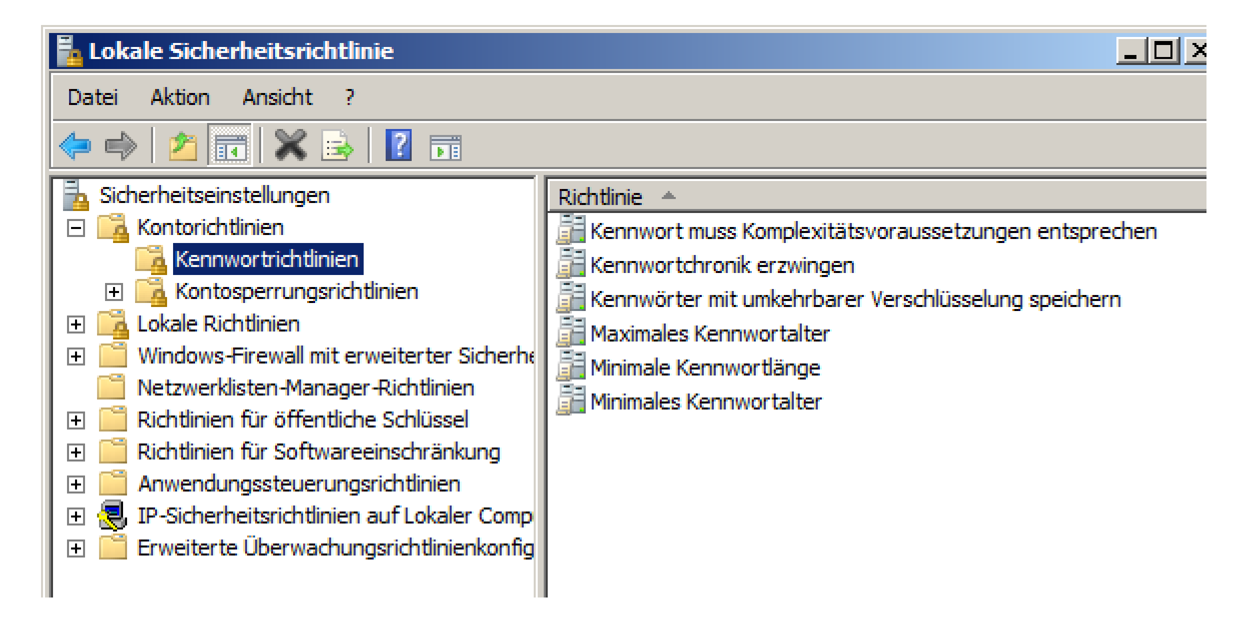
- Passwortalterung
  Passwörter sollten in regelmäßigen Abständen (spätestens alle 6 Monate) geändert werden.
- Mindestkomplexität
  Ein Passwort sollte eine Mindestkomplexität aufweisen, d.h. es soll den folgenden Anforderungen entsprechen:
  - Mindestlänge von 8 Zeichen
  - Mindestens 2 alphanumerische Zeichen und mindestens 1 Ziffer evtl. ein Sonderzeichen enthalten
- Passwort-Historie
  Ein neues Passwort muss sich signifikant vom vorhergehenden Passwort (alten Passwort) unterscheiden (mind. durch 3 Stellen).

Vorgehensweise

Die folgende Vorgehensweise wird am Beispiel des Betriebssystems "Windows 7" beschrieben.

Um die Passwortrichtlinien umzusetzen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Windows Startmenü und geben Sie im Suchfeld den Text "secpol.msc" ein.
   Die Anwendung "secpol.msc" wird in der Ergebnisliste angezeigt.
2. Klicken Sie auf die Anwendung "secpol.msc" in der Ergebnisliste.
   Geben Sie das Administratorenpasswort, falls dies erforderlich ist. Wenn Sie als Administrator angemeldet sind, bestätigen Sie die Ausführung der Anwendung.
   Der Dialog "Lokale Sicherheitsrichtlinie" wird geöffnet.
3. Wählen Sie "Kontorichtlinien > Kennwortrichtlinien" im linken Navigationsbereich des Dialog "Lokale Sicherheitsrichtlinie".
   Die Kennwortrichtlinien werden angezeigt.



4. Nehmen Sie die entsprechenden Einstellungen für die folgenden Richtlinien vor:

Richtlinie	Zweck
Kennwortchronik erzwingen	Verhindert, dass Benutzer ein neues Kennwort erstellen, das mit ihrem aktuellen oder einem kürzlich verwendeten Kennwort identisch ist. Der Wert "1" bedeutet beispielsweise, dass nur das letzte Kennwort als neues Kennwort verhindert wird. Der Wert "5" bedeutet, dass die letzten fünf Kennwörter als neues Kennwort verhindert werden.
Maximales Kennwortalter	Legt die maximale Gültigkeitsdauer von Kennwörtern in Tagen fest. Nach dieser Anzahl von Tagen muss der Benutzer das Kennwort ändern.
Minimales Kennwortalter	Legt fest, nach wie vielen Tagen ein Benutzer sein Kennwort frühestens ändern kann.
Minimale Kennwortlänge	Gibt die Mindestanzahl von Zeichen an, aus denen sich ein Kennwort zusammensetzt.
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Erfordert, dass ein Kennwort die folgenden Mindestanforderungen erfüllt: • Mindestens 6 Zeichen • Es muss sich aus Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen zusammensetzen • Darf nicht den Benutzernamen enthalten

5.5 Bedienberechtigungen – Rechteverwaltung des Bedieners

Die Strategie der aufgabenbezogenen Bedienungs- und Zugriffsrechte (role-based access control) beinhaltet die Einschränkung auf minimal benötigte Rechte und Funktionen der Benutzer, Bediener, Geräte, Netzwerk- und Software-Komponenten.

5.5.1 SIMATIC Logon

In Anlagen, die mit Prozessleitsystemen automatisiert sind, bestehen folgende spezielle/wichtige Anforderungen bezüglich des Zugriffs auf Funktionen, Daten und Anlagenbereiche:

- Benutzerverwaltung zur Erteilung von Zugriffsrechten, um unerlaubte oder ungewollte Zugriffe auf die Anlage zu vermeiden
- Erstellen und Archivieren von Nachweisen über wichtige oder kritische Handlungen

Mit SIMATIC Logon können SIMATIC-Applikationen und Anlagenbereichen individuelle, aufgabenbezogene Berechtigungen zugeordnet werden.

SIMATIC Logon unterstützt die Benutzerverwaltung auf lokalen Computern und in Windows-Domains. Es wird empfohlen, SIMATIC Logon im Active Directory in einer Domain zu verwenden, um die Vorteile der Funktionen der zentralen Gruppen- und Benutzerverwaltung zu nutzen.

SIMATIC Logon bietet die Funktion eines "Default Users". Dieser wird beim Start der PCS 7-Applikation oder beim Abmelden eines SIMATIC Logon-Benutzers automatisch angemeldet. Für dieses Benutzerkonto wird empfohlen,die minimale Anzahl der benötigten Benutzerrechte zuzuweisen, z. B. für die Notfallbedienung.

Die folgenden Applikationen haben eine Anbindung an die Komponenten von SIMATIC Logon:

- Automation License Manager
- WinCC
- SIMATIC Batch
- STEP 7

Detaillierte Informationen zu SIMATIC Logon finden Sie im Handbuch "SIMATIC Logon“ (http://support.automation.siemens.com/WW/view/de/34519648).

5.5.2 Zugriffsschutz für Projekte/Bibliotheken auf der Engineering Station

Einleitung

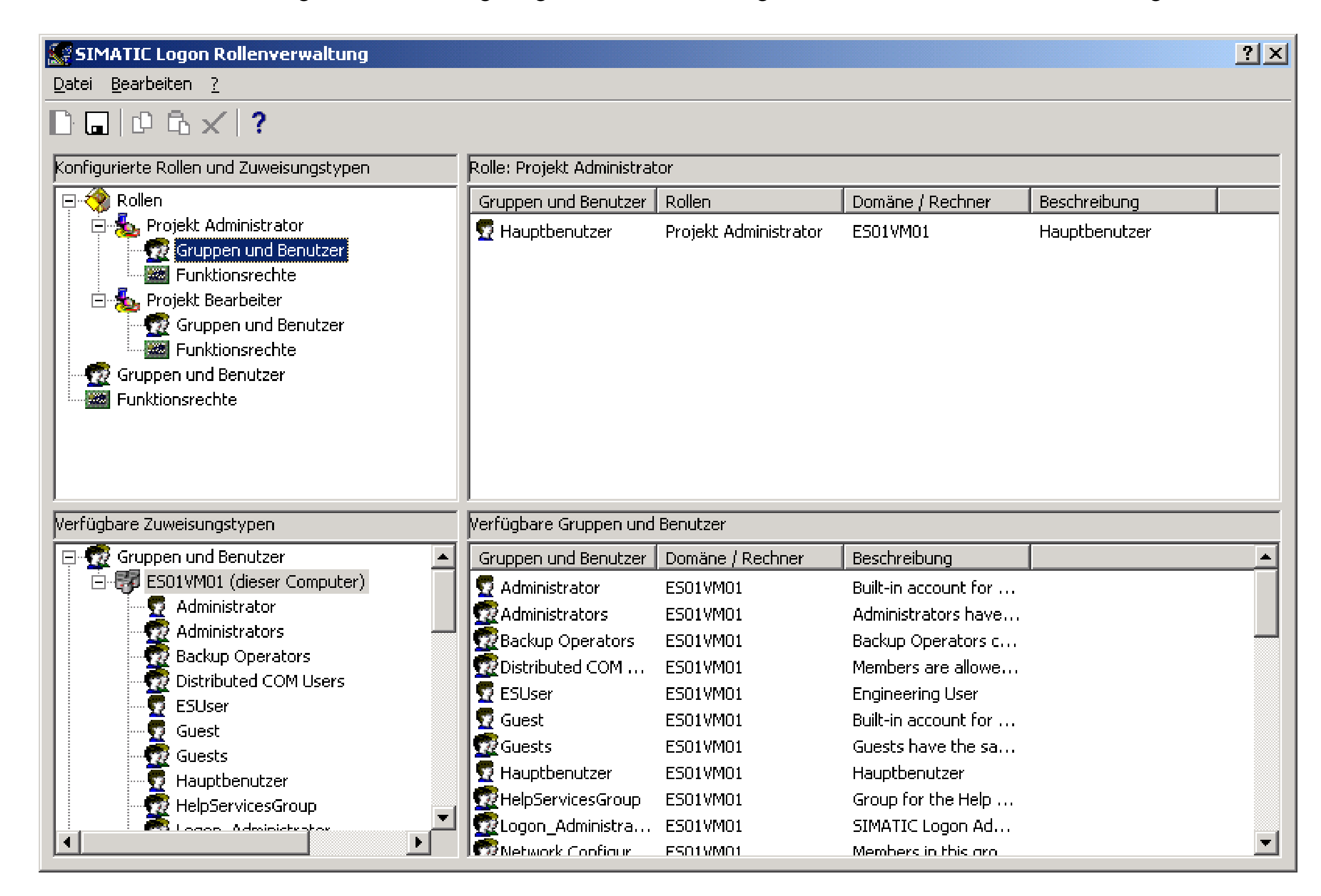
Es wird empfohlen, die Projekte und Bibliotheken vor ungewolltem Zugriff zu schützen und alle Zugriffe zu protokollieren. Dies setzt die Installation von SIMATIC Logon voraus. Die Software SIMATIC Logon definiert Benutzerrollen für das Engineering System und deren Zuordnung zu den definierten Windows-Benutzer/-gruppen.

Das Öffnen und Bearbeiten von zugriffsgeschützten Projekten und Bibliotheken ist dann nur noch für Windows-Benutzer möglich, die einer der folgenden Benutzerrollen zugehörig sind:

- Projekt-Administrator
- Projekt-Bearbeiter
- Beliebiger Bearbeiter, wenn dieser sich über das Projektpasswort authentifiziert hat

Der Benutzer mit der Rolle "Projekt Administrator" legt die Benutzer für die Rollen "Projekt Bearbeiter" und das Projektpasswort fest. Er ist berechtigt zum Aktivieren und Deaktivieren des Zugriffsschutzes. Der Projekt-Administrator kann Windows-Benutzer einer der beiden Benutzerrollen zuordnen.

Die folgende Abbildung zeigt den SIMATIC Logon-Editor für die Rollenverwaltung:



Einstellung des Zugriffsschutzes

Die folgenden Einstellungen für den Zugriffschutz sind im SIMATIC Manger pro Projekt und Bibliothek vorzunehmen. Der Abgleich über ein gesamtes Multiprojekt ist möglich.

Netzadressbereich	Beschreibung	Ausführbar mit Benutzerrolle
Zugriffsschutz aktivieren (inklusive Projektpasswort festlegen)	• Schaltet den Zugriffsschutz für ein bestimmtes Projekt bzw. eine bestimmte Bibliothek ein. Nur Windows-Benutzer, die der Benutzerrolle Projekt-Bearbeiter oder Projekt-Administrator zugeordnet sind, können dieses Projekt bzw. diese Bibliothek öffnen und bearbeiten. • Legt das Projektpasswort fest. Pro Projekt/pro Bibliothek kann ein Projektpasswort festgelegt werden.	Projekt-Administrator
Zugriffsschutz deaktivieren	Schaltet den Zugriffsschutz für ein bestimmtes Projekt bzw. eine bestimmte Bibliothek wieder aus	Projekt-Administrator
Benutzer verwalten	Legt die Projekt-Administratoren und Projekt-Bearbeiter fest	Projekt-Administrator
Zugriffsschutz im Multiprojekt abgleichen	Legt die Projekt-Administratoren und Projekt-Bearbeiter einheitlich für alle Projekte und Bibliotheken eines Multiprojektes fest	Projekt-Administrator
Änderungsprotokoll anzeigen	Öffnet das Änderungsprotokoll	Projekt-Administrator Projekt-Bearbeiter
Zugriffsschutz und Änderungsprotokoll entfernen	Entfernt den Zugriffsschutz und löscht das Änderungsprotokoll eines passwortgeschützten Projektes bzw. einer passwortgeschützten Bibliothek	Projekt-Administrator

Zugriffsschutz für Projekte/Bibliotheken aktivieren

Die folgenden Voraussetzungen müssen erfüllt sein:

- SIMATIC Logon ist installiert.
- In SIMATIC Logon sind durch die PCS 7-Installation die Benutzerrollen "Projekt Administrator" und "Projekt Bearbeiter" automatisch angelegt.
- Sie sind in SIMATIC Logon der Benutzerrolle "Projekt Administrator" zugeordnet.
- Sie sind als "Projekt Administrator" oder "Projekt Bearbeiter" angemeldet.

Der aktuell angemeldete Benutzer ("Projekt Administrator" oder "Projekt Bearbeiter") werden in der Statuszeile des SIMATIC Manager angezeigt. Beim erstmaligen Aktivieren des Zugriffsschutzes wird das Projektformat geändert. Aus diesem Grund erhalten Sie einen Hinweis, dass das geänderte Projekt nicht mehr mit älteren PCS 7-Versionen bearbeitet werden kann.

Um den Zugriffschutz für Projekte/Bibliotheken zu aktivieren und das Passwort zu ändern, gehen Sie folgendermaßen vor:

1. Selektieren Sie das Projekt bzw. die Bibliothek im SIMATIC Managers.
2. Wählen Sie den Menübefehl "Extras > Zugriffsschutz > Aktivieren".
3. Tragen Sie im Dialog "Zugriffsschutz aktivieren" das Passwort und die Passwortbestätigung ein.
4. Klicken Sie auf die Schaltfläche "OK".
   Das ausgewählte Projekt bzw. die Bibliothek wird durch ein Passwort geschützt und kann nur von autorisierten Benutzern zur Bearbeitung geöffnet werden.

Um den Zugriffschutz für Projekte/Bibliotheken zu deaktivieren, gehen Sie folgendermaßen vor:

1. Selektieren Sie das Projekt/die Bibliothek im SIMATIC Manager.
2. Wählen Sie den Menübefehl "Extras > Zugriffsschutz > Deaktivieren".
3. Tragen Sie im Dialog "Zugriffschutz deaktivieren" das Passwort und die Passwortbestätigung ein.
4. Klicken Sie auf die Schaltfläche "OK".
   Das ausgewählte Projekt bzw. die Bibliothek wird nicht mehr durch ein Passwort geschützt und kann von jedem Benutzer zur Bearbeitung geöffnet werden.

Weitere Informationen

Weitere Informationen finden Sie im Projektierungshandbuch "SIMATIC Prozessleitsystem PCS 7 Engineering System" (http://support.automation.siemens.com/WW/view/de/68157345).

5.5.3 Änderungen im Änderungsprotokoll dokumentieren

Einleitung

Im Änderungsprotokoll wird dokumentiert, welcher Benutzer zu welcher Zeit an welcher CPU welche Änderung aus welchem Grund vorgenommen hat.

Voraussetzung

Die folgenden Voraussetzungen müssen erfüllt sein:

- Der SIMATIC Logon Service ist installiert
- Der Zugriffsschutz ist aktiviert

Vorgehensweise

Um das Änderungsprotokoll für einen Ordner im SIMATIC Manager zu aktivieren, gehen Sie folgendermaßen vor:

1. Selektieren Sie in der Komponentensicht des SIMATIC Managers den Ordner, für den Sie das Änderungsprotokoll aktivieren möchten.
2. Wählen Sie den Menübefehl "Extras > Änderungsprotokoll > Aktivieren".
   Das Änderungsprotokoll ist für den gewählten Ordner aktiviert.

Im Änderungsprotokoll wird Folgendes protokolliert:

- Aktivierung/Deaktivierung/Konfiguration von Zugriffsschutz und Änderungsprotokoll
- Öffnen/Schließen von Projekten und Bibliotheken
- Laden ins Zielsystem (Systemdaten)
- Ausgewählte Operationen zum Laden und Kopieren von Bausteinen
- Aktivitäten zur Änderung des Betriebszustands
- Urlöschen

5.5.4 Änderungen im ES-Protokoll dokumentieren

Einleitung

Im ES-Protokoll wird dokumentiert, welcher Benutzer zu welcher Zeit an welcher CPU welche Änderungen aus welchem Grund durchgeführt hat. Wenn die Option "ES-Protokoll aktiv" aktiviert ist, werden im CFC/SFC (Objekte des Planordners) zusätzlich zu den abgesicherten Aktionen auch die Aktionen beim Laden und die aktuellen Zeitstempel protokolliert.

Voraussetzung

Die folgenden Voraussetzungen müssen erfüllt sein:

- Der SIMATIC Logon Service ist installiert
- Das Änderungsprotokoll ist aktiviert

Vorgehensweise

Um das ES-Protokoll zu aktivieren, gehen Sie folgendermaßen vor:

1. Selektieren Sie in der Komponentensicht des SIMATIC Managers den Planordner, für den Sie das ES-Protokoll aktivieren möchten.
2. Wählen Sie den Menübefehl "Bearbeiten > Objekteigenschaften".
   Das Dialogfeld "Eigenschaften Planordner" wird geöffnet.
3. Wechseln Sie zum Register "Erweitert".
4. Aktivieren Sie die Option "ES-Protokoll aktiv".
5. Klicken Sie auf die Schaltfläche "OK".

Im ES-Protokoll wird Folgendes protokolliert:

- Jede Aktion wird in einer Hauptzeile, gefolgt von den Zeilen des Grundes und dem Protokoll der Aktion (z. B. Ladeprotokoll), chronologisch fortlaufend protokolliert. Die letzte Aktion steht in der obersten Zeile.
- Bei der Aktion "Laden gesamtes Programm" wird das ES-Protokoll aus dem Protokoll gelöscht, gleichzeitig aber mit einer Datumskennung als Datei archiviert. Die Archivierungsaktion und der verwendete Dateiname (einschließlich Pfad) werden im Protokoll festgehalten.
- Bei der Aktion "Testmodus ein" werden alle folgenden Aktionen, die zu einer Veränderung (Wertänderung) in der CPU führen, protokolliert. Als Aktion wird protokolliert, welcher Wert wie geändert wurde (Adresse, alter Wert, neuer Wert). Das sind im Einzelnen:
  - Im CFC
Parametrierung von Anschlüssen
Forcen aktivieren/deaktivieren und Force-Wertänderungen
Ein-/Ausschalten von Ablaufgruppen
  - Im SFC
Parametrierungen von Konstanten in Schritten
Parametrierungen von Konstanten in Transitionen
Parametrierungen von Konstanten in Ketteneigenschaften

5.5.5 Zugriffsschutz bei Operator Stationen

Es muss gewährleistet sein, dass ein ausreichender Schutz vor unbefugten Zugriff auf die Operator Stationen vorhanden ist. Hierbei spielen zwei unterschiedliche Fallbeispiele eine Rolle:

- Zum einen muss die Operator Station vor unbefugten Zugriff wie z. B. Bedieneingriffe oder Bildanwahl geschützt werden, wenn an dieser Station niemand angemeldet ist. Das bedeutet, dass bei Abmeldung des Operators von der Station durch ziehen der Chipkarte oder manuell die Station in einen Zustand schalten muss, der es Unbefugten unmöglich macht, diese Station zu verwenden (Screen Saver Mode). Somit ist es nicht zulässig, dass ein aktuell angewähltes Bild nach dem Abmelden eines Bedieners weiterhin angezeigt wird.
- Zum anderen muss die Operator Station so "verriegelt" werden, dass es für einen Unbefugten unmöglich ist, den Desktop des Betriebssystems zu erreichen.

5.6 Schutzstufenkonzept

Durch die Verwendung einer Schutzstufe kann das Automatisierungsgerät vor unberechtigten Zugriff geschützt werden. Dabei stehen 3 verschiedene Schutzstufen in der CPU zur Verfügung:

Schutzstufe 1

Je nach Art der CPU wird diese Schutzstufe unterschiedlich benannt.

Bei Standard-CPUs mit Schlüsselschaltern heißt die Schutzstufe 1 "Schlüsselschalterstellung". Die Stellung des Schlüsselschalters (Betriebsartenschalter) der CPU bestimmt den Schutz:

- Schlüsselschalter in Stellung RUN-P oder STOP: keine Einschränkungen
- Schlüsselschalter in Stellung RUN: nur lesender Zugriff möglich

Durch Passworteingabe können Sie den Schlüsselschalter-Schutz umgehen.

Bei Standard-CPUs, deren Betriebsartenschalter nicht als Schlüsselschalter ausgeführt ist, sondern als RUN-STOP-Schalter heißt die Schutzstufe 1 "kein Schutz". Eine Passworteingabe ist hier nicht möglich.

Bei F-CPUs bzw. H-CPUs heißt die Schutzstufe 1 "Zugriffschutz für F-CPU oder Schlüsselschalterstellung". In der Voreinstellung kann kein Sicherheitsprogramm geladen werden. Erst durch Vergabe eines Passwortes und durch die Option "CPU enthält Sicherheitsprogramm" können Sie Sicherheitsbausteine in die CPU laden.

Schutzstufe 2: Schreibschutz

Bei Schutzstufe 2 ist nur lesender Zugriff auf die CPU möglich, unabhängig von der Stellung des Schlüsselschalters.

Schutzstufe 3: Schreib-/Leseschutz

Bei Schutzstufe 3 ist weder lesender noch schreibender Zugriff auf die CPU möglich, unabhängig von der Stellung des Schalters.

Hinweis

Schutz vor unberechtigten Zugriff

Die Verwendung der Schutzstufe 3 "Schreib-/Leseschutz" zum Schutz vor unberechtigten Zugriff auf das Automatisierungssystem (CPU) wird empfohlen.

Verhalten einer passwortgeschützten CPU im Betrieb

Vor der Ausführung einer Online-Funktion wird die Zulässigkeit geprüft und ggf. zur Passworteingabe aufgefordert.

Beispiel: Die Baugruppe wurde mit Schutzstufe 2 parametriert und Sie wollen die Funktion "Variable steuern" ausführen. Da es sich um einen schreibenden Zugriff handelt, muss zur Ausführung der Funktion das parametrierte Passwort eingegeben werden.

Weitere Informationen

Weitere Informationen zum Schutzstufenkonzept finden Sie im Handbuch "SIMATIC Prozessleitsystem PCS 7 Engineering System“ (http://support.automation.siemens.com/WW/view/de/68157345).

Patchmanagement 6

6.1 Übersicht

Microsoft beseitigt regelmäßig Sicherheitslücken in seinen Produkten und stellt diese Korrekturen über offizielle Updates/Patches seinen Kunden zur Verfügung.

Um einen sicheren und stabilen Betrieb von SIMATIC PCS 7 zu gewährleisten, ist die Installation von "Sicherheitsupdates" und "Wichtigen Updates" notwendig.

Zur Implementierung dieser Updates bestehen grundsätzlich zwei Möglichkeiten:

- Windows Updates über einen WSUS
  Bereitstellung von Windows Updates für alle Rechner des Automatisierungssystems durch einen separaten Windows Server Update Service (WSUS)
- Manuelles Update
  Manuelle Installation der "Sicherheits-Updates" und "Wichtigen Updates" nach einem Download von den Microsoft Sites auf allen Rechnern des Automatisierungssystems.

Informationen zum Thema "Patchmanagement" finden Sie in den folgenden Dokumenten:

- Handbuch "SIMATIC Prozessleitsystem PCS 7 Patchmanagement und Securityupdates“ (http://support.automation.siemens.com/WW/view/de/38621083)
- FAQ "Wie kann man herausfinden, welche Microsoft Patches auf dem PC installiert sind?“ (http://support.automation.siemens.com/WW/view/de/48844294)
- FAQ "Welche Microsoft Patches ("Sicherheitsupdates" und "Wichtige Updates") sind bei SIMATIC PCS 7 auf Verträglichkeit getestet?“ (http://support.automation.siemens.com/WW/view/de/22754447)

Informationen zu Microsoft Updates und dem WSUS finden Sie auf den folgenden Microsoft-Seiten:

- http://www.microsoft.com/germany/technet/servicedesk/bulletin/default.mspx
- http://www.microsoft.com/wsus

Unterstützung bei der Umsetzung bzw. Implementierung eines Patchmanagement in Ihre Anlage erhalten Sie bei den Industrial Security Services. Weitere Informationen und die entsprechenden Ansprechpartner finden Sie unter folgender Adresse:

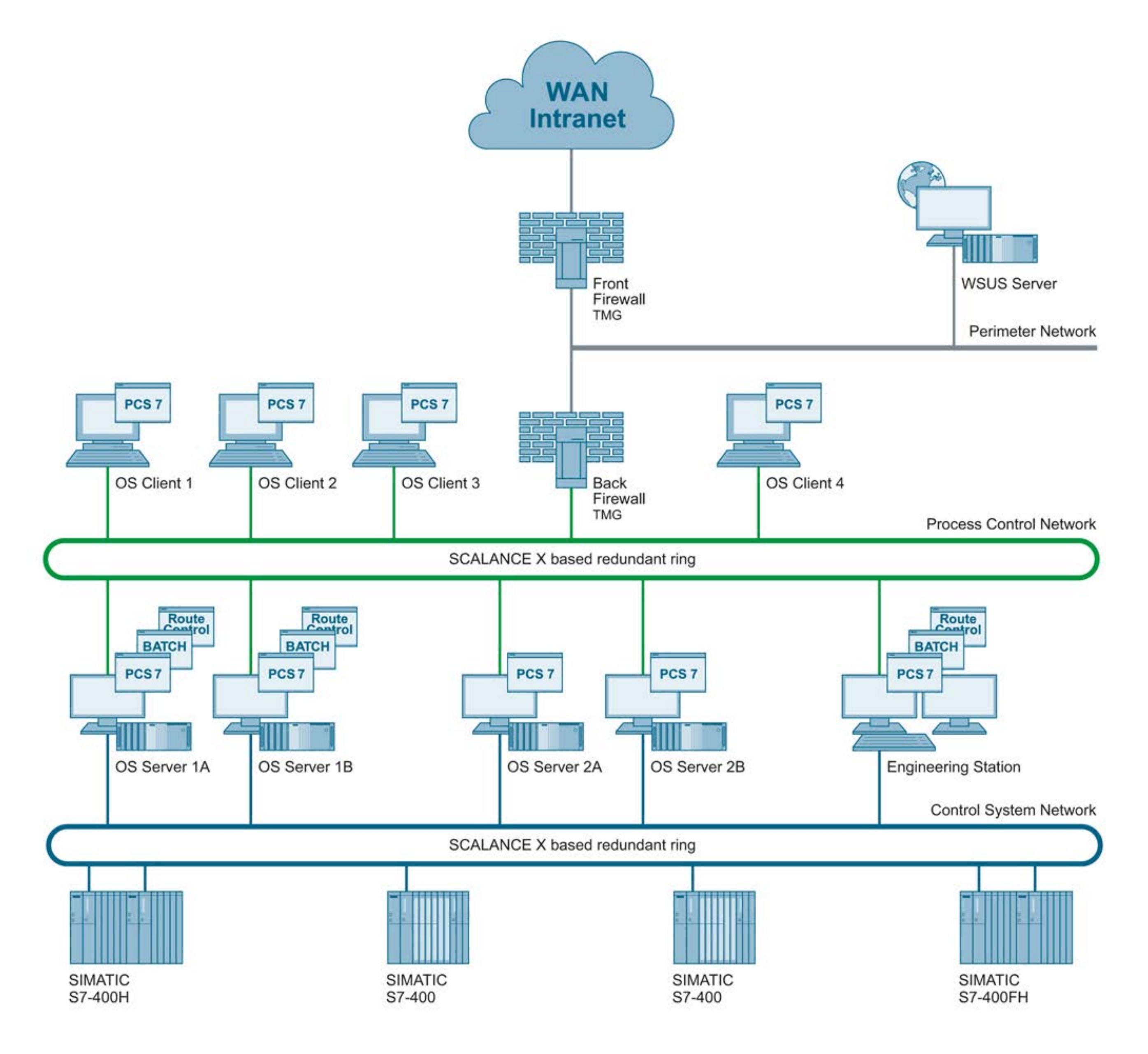
- http://www.industry.siemens.com/topics/global/de/industrial-security/seiten/default.aspx

Sie können Ihre Anfrage per E-Mail auch direkt an "industrialsecurity.i@siemens.com" richten.

6.2 Windows Server Update Service (WSUS)

WSUS-Server

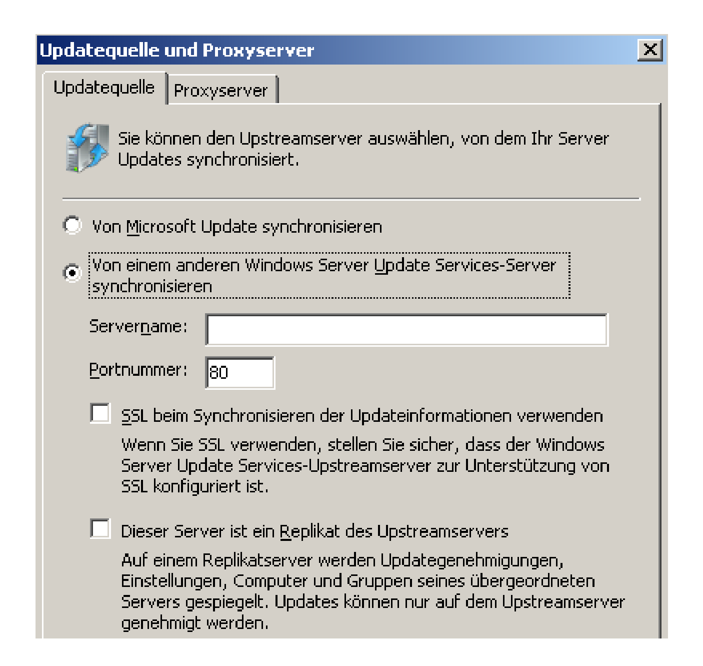
Der WSUS-Server ist entsprechend den Regeln zur Aufteilung der Komponenten in Sicherheitszellen in einem separaten Netzwerk (Perimeter-Netzwerk / DMZ) zu separieren. Für das Patchmanagement bzw. den WSUS-Server können alle Lösungen bezüglich der Sicherung der Zugriffspunkte zu den Sicherheitszellen wie z. B. Front/Back Firewall oder Treehomed Firewall verwendet werden. Bei der Konfiguration der Zugriffsregeln für die Back Firewall bzw. die Treehomed Firewall ist der WSUS im Perimeter-Netzwerk mittels Industrial Wizard zu konfigurieren.



Updatequelle

Für den WSUS-Server kann entweder ein vorhandener WSUS in einem übergeordneten, externen Netzwerk wie z. B. Betriebsnetzwerk oder Corporate-Netzwerk oder aber Microsoft Update im Internet zur Synchronisierung eingestellt werden. Die Entscheidung hat einerseits Auswirkungen auf die Konfiguration der Firewall (Frontfirewall bzw. Treehomed Firewall), andererseits auf die Konfiguration des WSUS-Servers.

In der WSUS Konfiguration muss die entsprechende Update-Quelle eingestellt werden:



6.2.1 Empfohlene Vorgehensweise zum Patchmanagement mit dem Microsoft Windows Server Update Service (WSUS)

Voraussetzung

Ein WSUS ist für Ihre PCS 7-Anlage eingerichtet.

WSUS konfigurieren

Um den WSUS zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die WSUS-Verwaltungskonsole und klicken Sie auf "Optionen".
2. Wählen Sie im Dialog "Produkte und Klassifikationen" im Register "Produkte" alle für die Anlage relevanten Microsoft-Produkte aus.

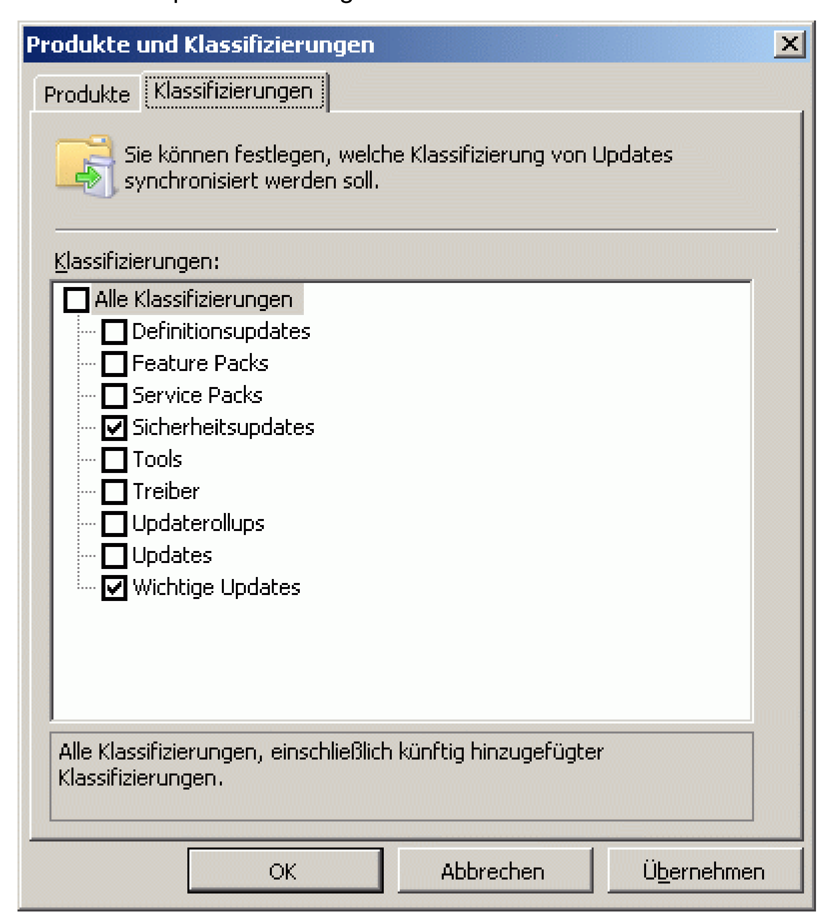
Hinweis

Informationen über die zulässigen Microsoft-Patches finden Sie in der folgenden FAQ:

Welche Microsoft Patches ("Sicherheitsupdates" und "Wichtige Updates") sind bei SIMATIC PCS 7 auf Verträglichkeit getestet?
(http://support.automation.siemens.com/WW/view/de/18490004)

---

3. Wählen Sie unter "Produkte und Klassifikationen" die "Wichtige Updates" und "Sicherheitsupdates" im Register "Klassifikationen" aus.

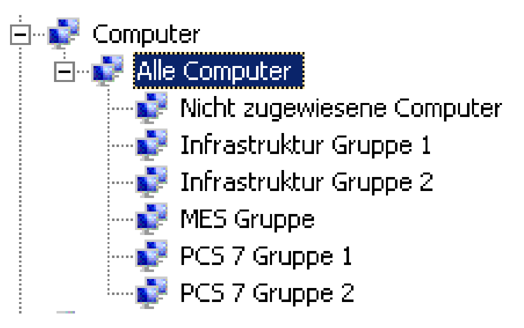


Hinweis

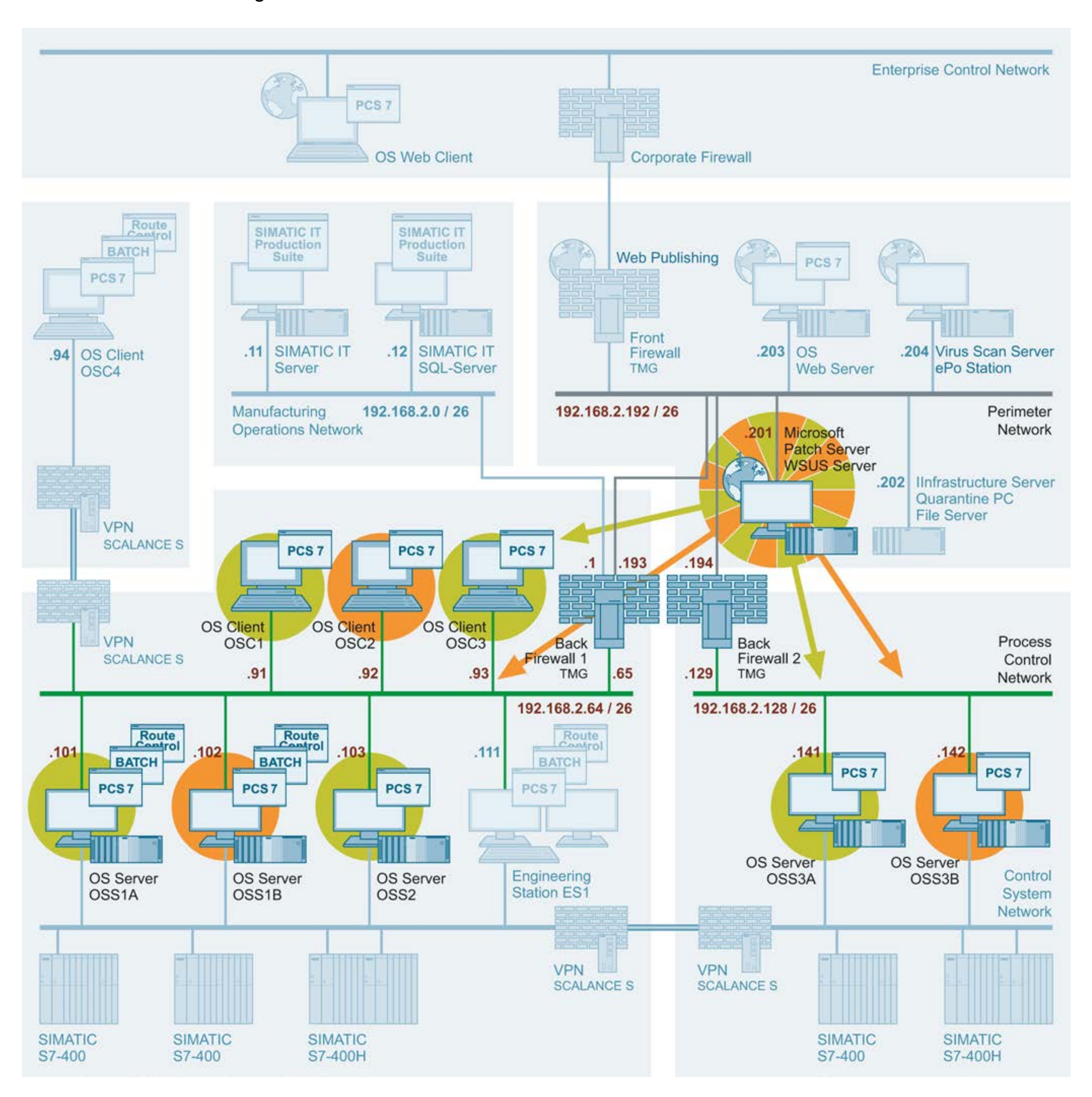
Beim Einsatz einer Industrial Automation Firewall 200/1000 bzw. Microsoft Forefront Threat Management Gateway (TMG) müssen zusätzlich auch die "Definitionsupdates" unter "Produkte und Klassifizierungen" ausgewählt werden.

---

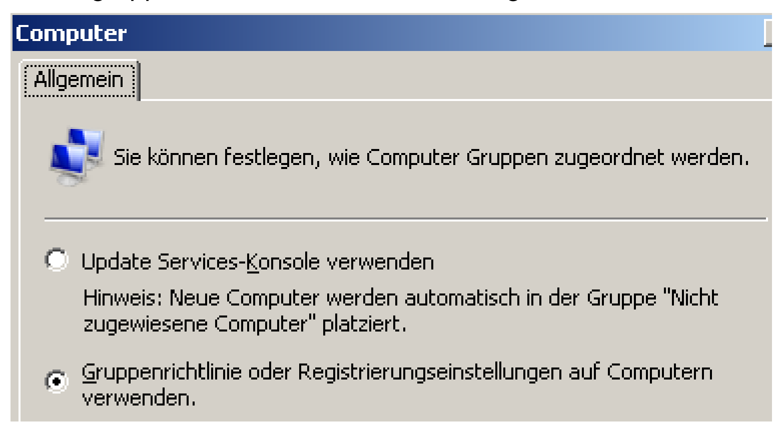
4. Legen Sie projektspezifische Gruppen für die Verteilung der Updates in die Anlage entsprechend dem Redundanzkonzept an und weisen Sie diesen Rechnergruppen die einzelnen Rechnersysteme zu.



Beispielsweise kann der Rechnergruppe "PCS 7 Gruppe 1" die OS-Server "OSS1A", "OSS2" und "OSS3A" sowie die OS-Clients "OSC1" und "OSC3" und der Rechnergruppe "PCS 7 Gruppe 2" die OS-Server "OSS1B" und "OSS3B" sowie der OS-Client "OSC2" zugeordnet werden.



Damit die Rechner direkt den richtigen Rechnergruppen zugeordnet werden, ist die folgende Option einzustellen, unabhängig davon, ob die Verwaltung mittels Windows Arbeitsgruppen oder mittels Domains erfolgt.



Updates überprüfen

Um die Updates zu überprüfen, gehen Sie folgendermaßen vor:

1. Laden Sie die Excel-Tabelle aus der folgenden FAQ auf ihren Rechner:
   – Welche Microsoft Patches ("Sicherheitsupdates" und "Wichtige Updates") sind bei SIMATIC PCS 7 auf Verträglichkeit getestet? (http://support.automation.siemens.com/WW/view/de/22754447)
2. Öffnen Sie die Tabelle und filtern Sie in der Spalte "Test Result" auf "failed".
3. Überprüfen Sie die Spalte "Comment", ob diese Updates ersetzt wurden

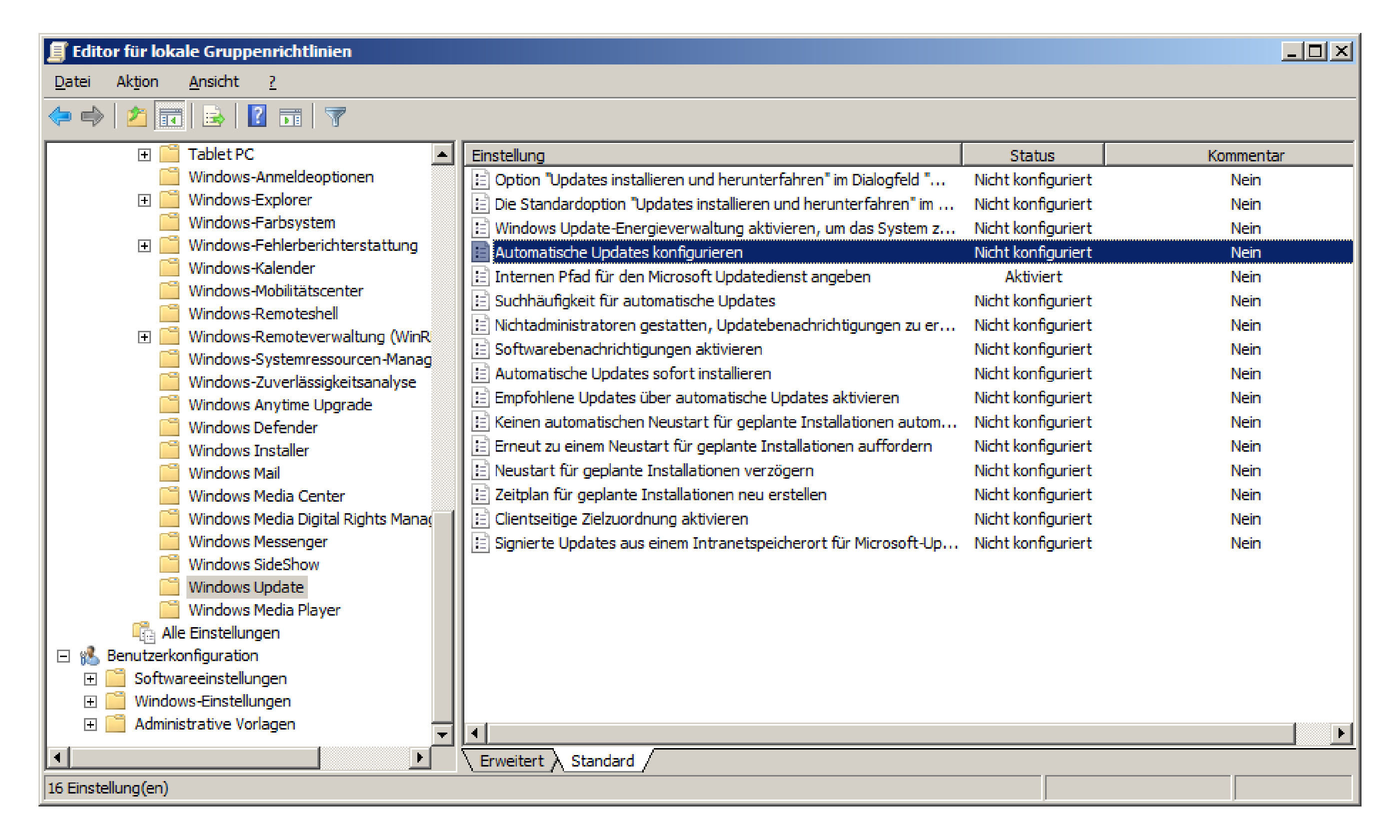
WSUS-Administration

1. Selektieren Sie alle verfügbaren Updates in den Kategorien "Wichtige Updates" und "Sicherheitsupdates" und geben Sie diese zur Installation in den angelegten Gruppen frei.
2. Melden Sie sich auf den mit dem WSUS verbundenen Clients mit einem administrativen Account an (die Clients wurden entsprechend konfiguriert, um die Updates vom WSUS zu erhalten).
3. Führen Sie die angebotenen Updates aus.

6.2.2 Konfiguration der Computerrichtlinien

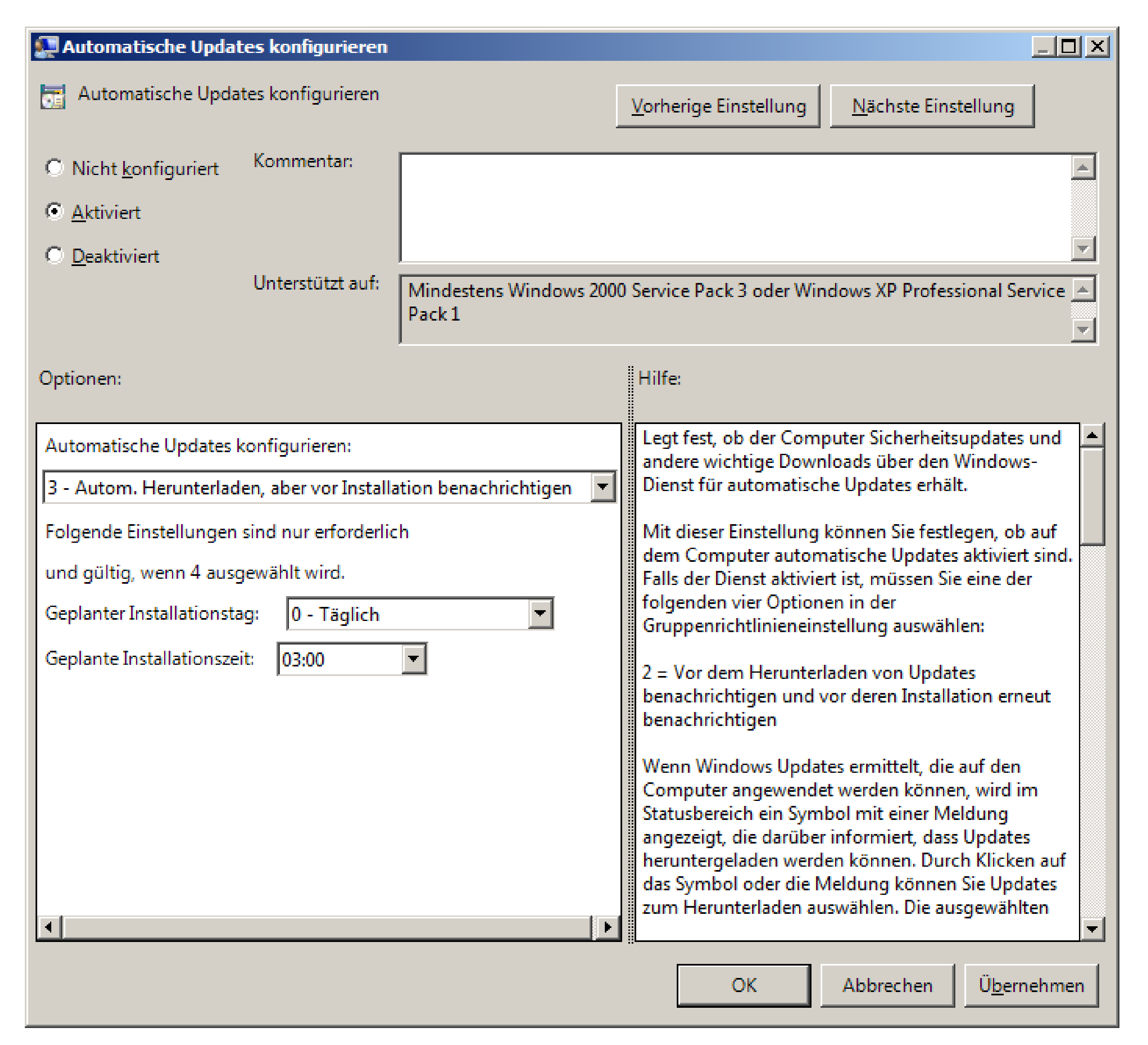
Die Richtlinien für den Windows Update-Dienst werden über den Editor für lokale Gruppenrichtlinien eingestellt. Bei der Verwendung eines Domain-Controllers werden die Einstellungen zentral durchgeführt und entsprechend auf alle Rechnersysteme verteilt. Wenn die Verwaltung mittels Windows-Arbeitsgruppen erfolgt, müssen diese Einstellungen auf jedem Rechner separat durchgeführt werden.

Die folgende Abbildung zeigt den Editor für lokale Gruppenrichtlinien:

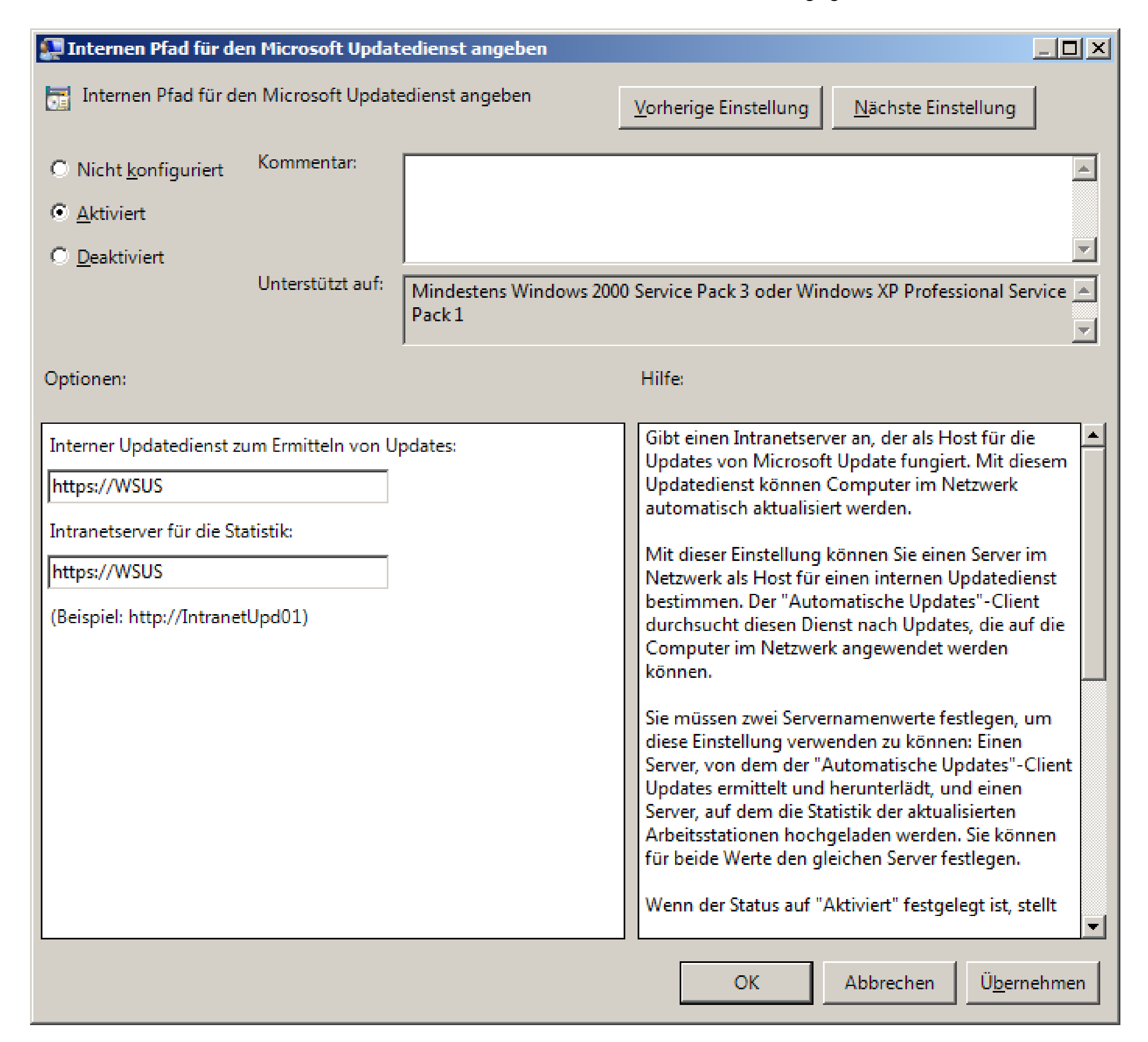


Die folgenden Gruppenrichtlinien müssen konfiguriert werden:

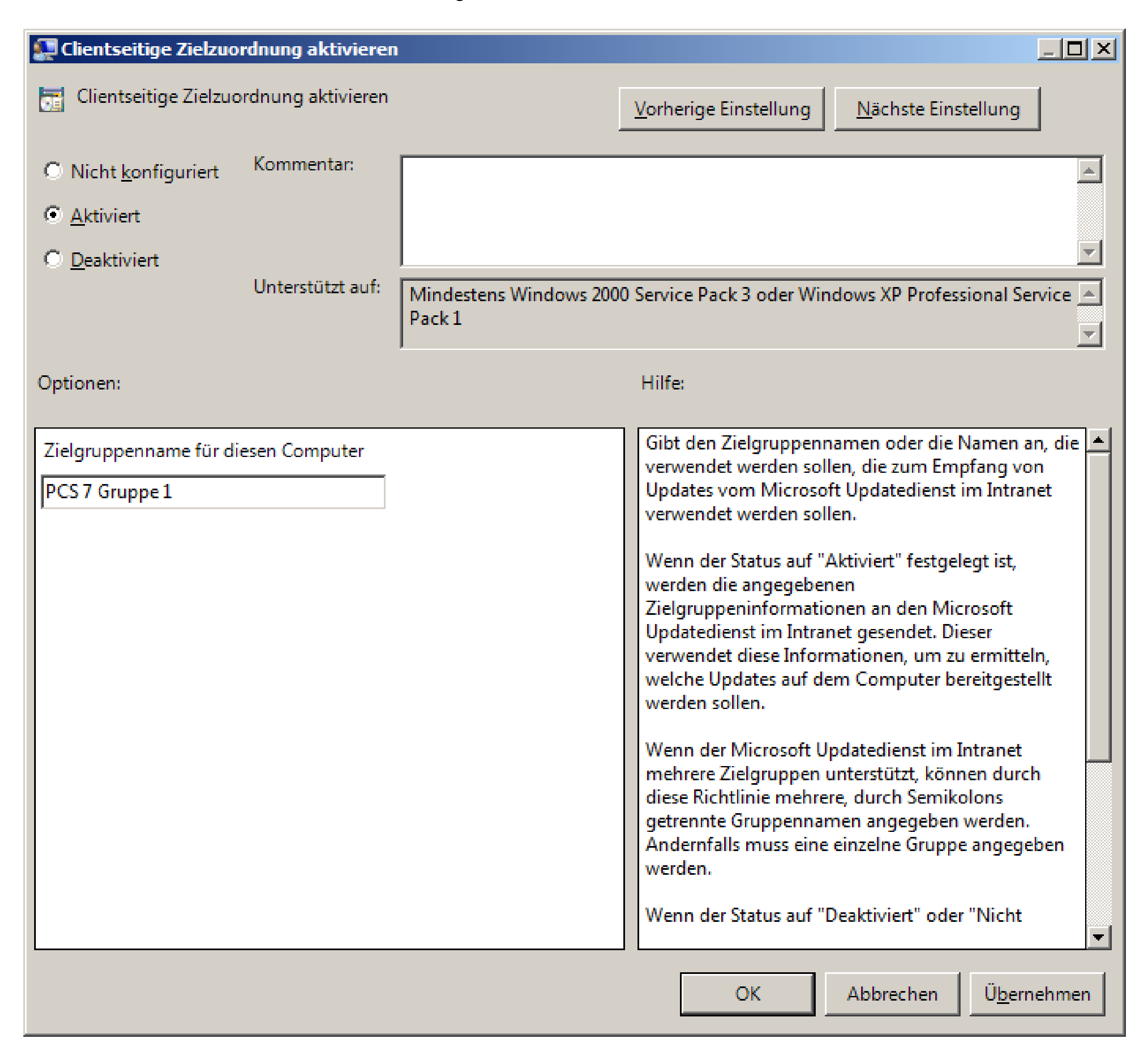
- Richtlinie "Automatische Updates konfigurieren"
  Die Richtlinie "Automatische Updates konfigurieren" muss aktiviert werden. Im Eigenschaftsdialog der Richtlinie muss eingestellt werden, dass Updates automatisch heruntergeladen aber nicht installiert werden dürfen.



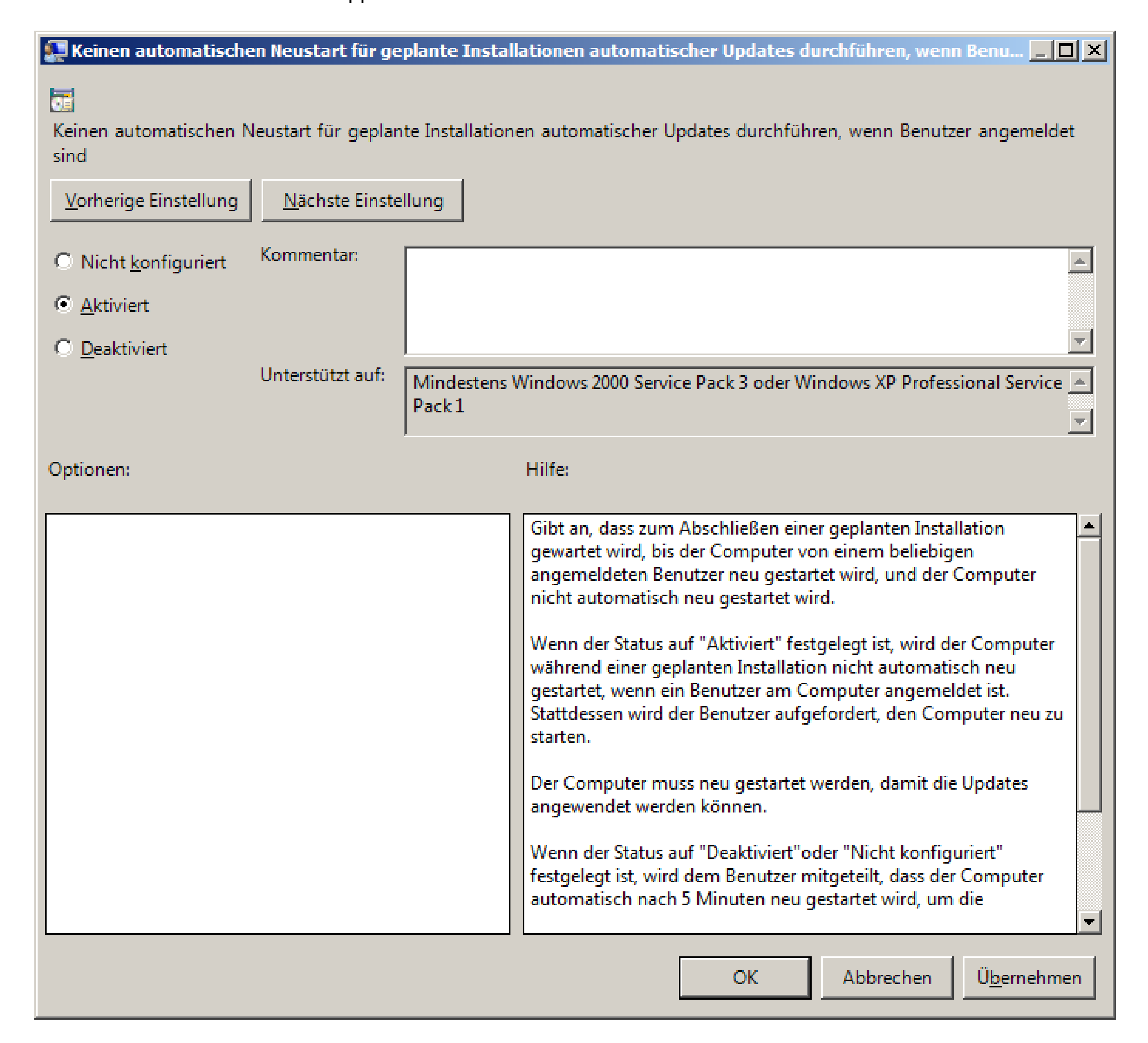
- Richtlinie "Internen Pfad für den Microsoft Updatedienst angeben"
  Die Richtlinie "Internen Pfad für den Microsoft Updatedienst angeben" muss aktiviert werden. Im Eigenschaftsdialog dieser Richtlinie muss für den Fall, dass ein separater "Upstreamserver" in einem übergeordneten, externen Netzwerk verwendet wird, die IP-Adresse bzw. der Rechnername dieses WSUS Server angegeben werden.



- Richtlinie "Clientseitige Zielzuordnung aktivieren"
  Die Richtlinie "Clientseitige Zielzuordnung aktivieren" muss aktiviert werden. Im Eigenschaftsdialog der Richtlinie muss die Rechner-Gruppe eingegeben werden, zu welcher der Rechner gehören soll.



- Richtlinie "Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind"
  Diese Gruppenrichtlinie muss aktiviert werden.



6.2.3 Firewall-Regeln

Für den Zugriff des WSUS-Servers im Perimeter-Netzwerk über die Back Firewall bzw. Treehomed Firewall auf die Rechner im PCN ergeben sich die folgenden Zugriffsregeln:

- Zugriffsregeln zwischen dem WSUS-Server und einem Rechner im PCN

Name	Action	Protocols	From	To
Perimeter WSUS to PCN ... #1	Allow	HTTP HTTPS	IP-Adresse des WSUS-Servers	IP Adresse des Clients
PCN … to Perimeter WSUS #1	Allow	HTTP HTTPS	IP-Adresse des Client	IP Adresse des WSUS-Server

Für den Zugriff des WSUS-Servers im Perimeter-Netzwerk über die Front Firewall bzw. Treehomed Firewall auf das externe Netzwerk zum Download der Sicherheits- und der kritischen Updates wird die folgenden Zugriffsregeln benötigt:

- Zugriffsregeln für Firewall-Regel zum Update über die Microsoft-Seiten

Name	Action	Protocols	From	To
Allow Windows Update access to WSUS or External	Allow	HTTP HTTPS	IP-Adresse des WSUS-Servers	Microsoft Update Sites *.download.windowsupdate.com *.update.microsoft.com *.windowsupdate.com *.windowsupdate.microsoft.com

- Zugriffsregeln zum Update über einen übergeordneten WSUS-Server

Name	Action	Protocols	From	To
Allow Windows Update access to WSUS or External	Allow	HTTP HTTPS	IP-Adresse des WSUS-Servers	IP-Adresse des übergeordneten WSUS- Server

---

Hinweis

Das komplette Angebot zur Automation Firewall finden Sie im PCS 7 Add on-Katalog. Diesen Katalog können Sie über die SIMATIC PCS 7 Webseite (https://www.automation.siemens.com/mcms/process-control-systems/de/simatic-pcs-7/Pages/simatic-pcs-7.aspx) herunterladen.

6.3 Manuelles Update

Beim manuellen Update müssen die erforderlichen Updates zuerst über das Microsoft Download Center auf einen beliebigen Rechner heruntergeladen werden. Dabei ist auf die entsprechende Betriebssystem-Version (Server-Betriebssystem, Windows XP oder Windows 7) zu achten.

Nach dem Download und ggf. einem Transfer der Updates auf die Zielsysteme müssen die Updates separat installiert werden. Bei einem OS-Server oder OS-Client muss vor der Installation die Prozessführung (WinCC Runtime) beendet werden.
Starten Sie das Setup und folgen Sie den Anweisungen auf dem Bildschirm. Nach der Installation kann ein Neustart notwendig werden.

Hinweis

Diese Leitlinie gilt erst ab der Version PCS 7 V6.1 SP1.
Das oben beschriebene Vorgehen gilt nicht für neue Microsoft Service Packs, deren Einsatz nach wie vor einer expliziten Freigabe bedarf. Wenn die Updates einen höheren Versionsstand der Microsoft Software voraussetzen, vergewissern Sie sich über die PCS 7 Liesmich oder das Kompatibilitäts-Tool (http://support.automation.siemens.com/WW/view/de/2334224), dass diese höheren Software-Versionen oder Service Packs für SIMATIC PCS 7 freigegeben sind.

Schutz vor Schadsoftware mittels Virenscanner 7

7.1 Übersicht

Einleitung

In diesem Kapitel steht der Schutz des Automatisierungssystems bzw. der Rechner des Automatisierungssystems vor Schadsoftware im Mittelpunkt. Als Schadsoftware, Schadprogramm oder Malware werden Rechnerprogramme bezeichnet, die entwickelt wurden, um unerwünschte und ggf. schädliche Funktionen auszuführen. Hierbei unterscheidet man die folgenden Typen:

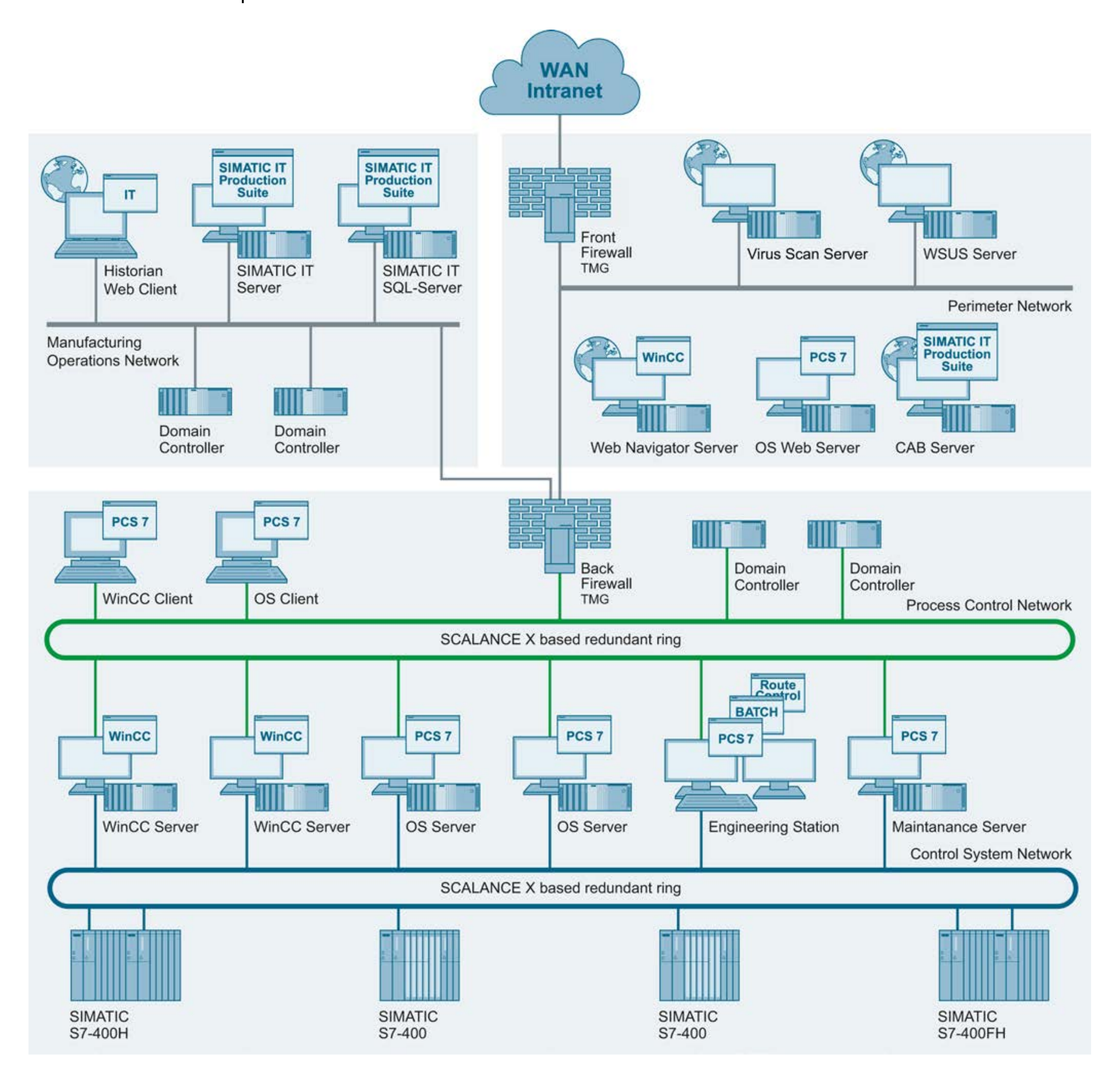
- Computerviren
- Computerwurm
- Trojanisches Pferd
- Sonstige potentiell, gefährliche Programme, z. B.:
  - Backdoor
  - Spyware
  - Adware
  - Scareware
  - Grayware

Ein Virenscanner oder Antivirenprogramm ist eine Software, die bekannte Schadsoftware aufspürt, blockiert und gegebenenfalls beseitigt.

Der Einsatz eines Virenscanners auf den Rechnern eines Automatisierungssystems darf den Prozessbetrieb einer Anlage nicht beeinträchtigen. Die folgenden zwei Beispiele zeigen die Problematik, die durch den Einsatz von Virenscannern in der Automatisierung entsteht:

- Ein Rechner darf auch bei Infektion durch Schadsoftware von einem Virenscanner nicht abgeschaltet werden, wenn dadurch die Kontrolle über die Produktionsanlage verloren geht (z. B. bei einem OS-Server).
- Auch eine durch Schadsoftware "infizierte" Projektdatei (z. B. ein Datenbankarchiv) darf nicht automatisch in die Quarantäne verschoben, blockiert oder gelöscht werden.

Für die Realisierung dieser Forderung wird die folgende Virenscanner-Architektur empfohlen:



Der Virenscan-Server ist ein Rechner, der Virenscan-Clients zentral verwaltet, Virensignaturdateien (Virenpattern) aus dem Internet vom Virenscan Hersteller lädt und diese auf die Virenscan Clients verteilt. Der Virenscan-Client ist ein Rechner, der auf Schadsoftware überprüft wird und vom Virenscan-Server verwaltet wird. D.h. PCS 7 OS-Server und OS-Clients sowie Batch-Server und Batch-Clients sind ebenso Virenscan-Clients wie Engineering Stationen oder auch Maintenance-Server.

Der Virenscan-Server ist, entsprechend den Regeln zur Aufteilung der Komponenten in Sicherheitszellen, in einem zusätzlichen Netzwerk (Perimeter-Netzwerk / DMZ) zu separieren. Für den Virenscan-Server können alle Lösungen bezüglich der Sicherung der Zugriffspunkte zu den Sicherheitszellen wie z.B. Front/Back Firewall oder Treehomed Firewall verwendet werden. Bei der Konfiguration des Regelsatzes für die Back Firewall bzw. die Treehomed Firewall ist der Virenscan-Server im Perimeter-Netzwerk entsprechend mittels des Industrial Wizards zu konfigurieren.

Update-Quelle

Für den Virenscan-Server kann entweder ein vorhandener Virenscan-Server in einem übergeordneten, externen Netzwerk z. B. Betriebsnetzwerk oder Corporate Netzwerk oder aber die URL des Virenscan Provider im Internet zur Synchronisierung eingestellt werden. Die Entscheidung hat einerseits Auswirkungen auf die Konfiguration der Firewall (Front Firewall bzw. Treehomed Firewall), andererseits auf die Konfiguration des Virenscan Servers.

Firewall-Regeln

Für den Zugriff des Virenscan-Servers im Perimeter-Netzwerk über die Back Firewall bzw. Treehomed Firewall auf die Virenscan-Clients im PCN ergeben sich die folgenden Firewall-Regeln.

- Beispiel für Firewall-Regeln zwischen einem Virenscan-Server und einem Virenscan-Client:

Name	Action	Protocols	From	To
Perimeter Virenscan-Server to PCN ... #1	Allow	HTTP HTTPS McAfee	IP-Adresse des Virenscan-Servers	IP-Adresse des Virenscan-Client
PCN … to Perimeter Virenscan-Server #1	Allow	HTTP HTTPS McAfee	IP-Adresse des Virenscan-Client	IP-Adresse des Virenscan-Servers

Für den Zugriff des Virenscan Server im Perimeter-Netzwerk über die Front Firewall bzw. Treehomed Firewall auf das externe Netzwerk zum Download der Virensignaturdateien werden folgende Firewall-Regeln benötigt:

- Beispiel für Firewall-Regeln zum Update der Virensignaturdateien per URL vom Provider

Name	Action	Protocols	From	To
Allow Virus Pattern Update access to overlapped Pattern Update Server or External	Allow	FTP over HTTP HTTPS	IP-Adresse des Virenscan-Servers	PatternUpdateSet ftp://ftp.nai.com http://update.nai.com

- Beispiel für Firewall-Regel zum Update der Virensignaturdateien von einem übergeordneten Virenscan-Server

Name	Action	Protocols	From	To
Allow Virus Pattern Update access to overlapped Pattern Update Server or External	Allow	FTP over HTTP HTTPS	IP-Adresse des Virenscan-Servers	PatternUpdateSet ftp://ftp.nai.com http://update.nai.com

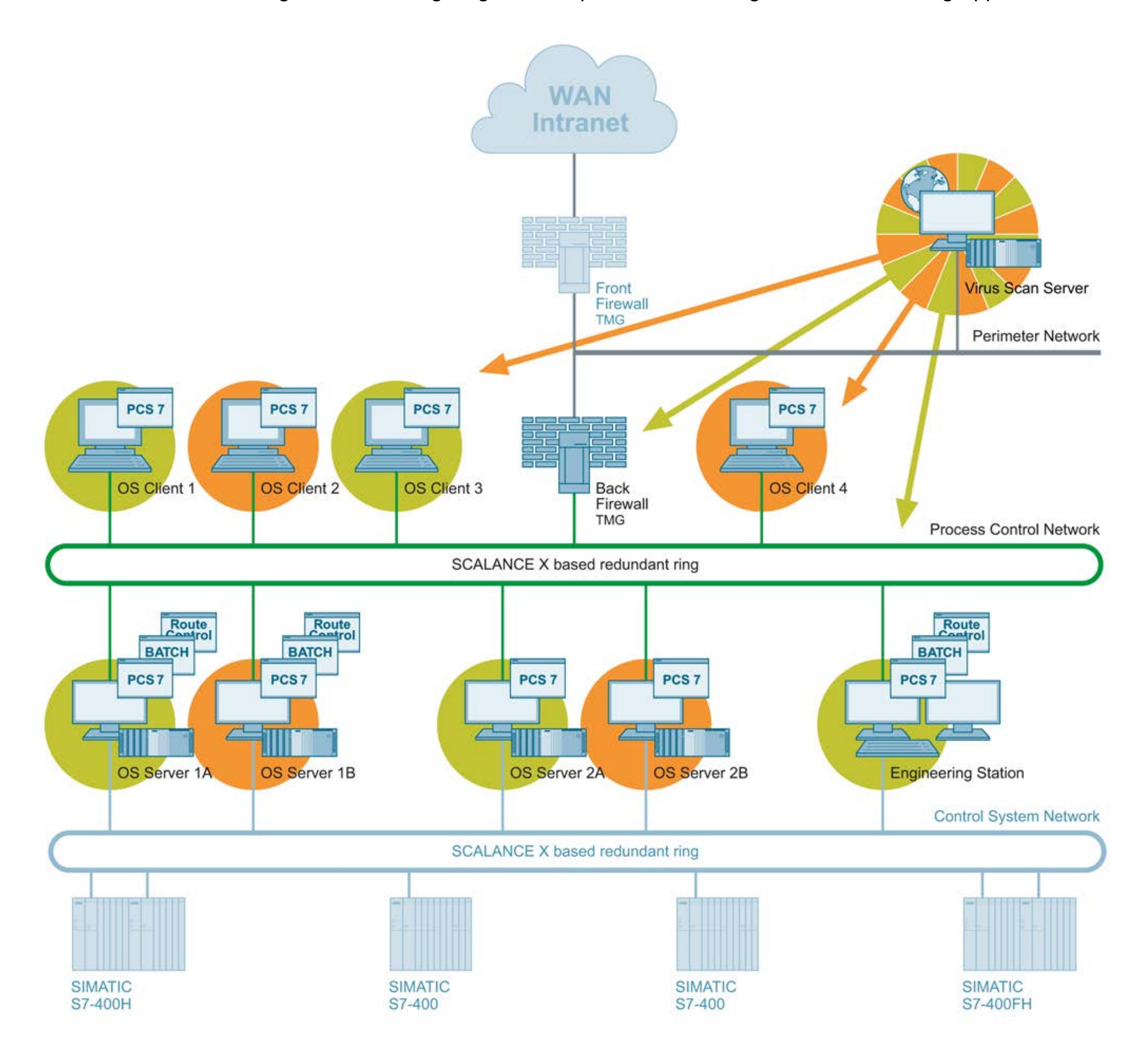
Hinweis

Das komplette Angebot zur Automation Firewall finden Sie im PCS 7 Add on-Katalog. Diesen Katalog können Sie über die SIMATIC PCS 7 Webseite (https://www.automation.siemens.com/mcms/process-control-systems/de/simatic-pcs-7/Pages/simatic-pcs-7.aspx) herunterladen.

Verteilung der Virensignaturdateien

Zur Verteilung der Virensignaturdateien vom Virenscan-Server auf die Virenscan-Clients wird empfohlen, projektspezifische Rechnergruppen zu bilden (analog der Rechnergruppen beim Patchmanagement).

Die folgende Abbildung zeigt ein Beispiel für die Bildung von zwei Rechnergruppen:



Weitere Informationen

Weitere Informationen zum Thema "Schutz vor Schadsoftware mittels Virenscanner" finden Sie in den folgenden Dokumenten:

- Handbuch "SIMATIC Prozessleitsystem PCS 7 Administration von Virenscannern" (http://support.automation.siemens.com/WW/view/de/38625951)
- FAQ "Welche Kompatibilität besitzt SIMATIC PCS 7 V8.x, V7.x, V 6.x, V5.x und V4.x?" (http://support.automation.siemens.com/WW/view/de/2334224)

Des Weiteren finden Sie im Industry Online Portal die Konfigurationsbeschreibungen für die unterschiedlichen Virenscanner:

- Konfiguration McAfee VirusScan (V8.5; V8.5i; V8.7) (http://support.automation.siemens.com/WW/view/de/38006821)
- Konfiguration McAfee VirusScan Enterprise 8.8 (http://support.automation.siemens.com/WW/view/de/66475606)
- Konfiguration Trend Micro OfficeScan 10.6 (http://support.automation.siemens.com/WW/view/de/59569279)
- Konfiguration Trend Micro OfficeScan V8.0 (http://support.automation.siemens.com/WW/view/de/38006929)
- Konfiguration Trend Micro OfficeScan V7.3 incl. Patch 2 (http://support.automation.siemens.com/WW/view/de/38006151)
- Konfiguration Symantec AntiVirus V10.2 (http://support.automation.siemens.com/WW/view/de/38006339)
- Konfiguration Symantec Endpoint Protection 11.0 (http://support.automation.siemens.com/WW/view/de/38004530)

7.2 Vorgehensweise nach einer Virusinfektion

Einleitung

Für den Fall einer Virusinfektion kann keine allgemeingültige Vorgehensweise empfohlen werden. Vielmehr muss bei einer solchen Infektion das Vorgehen zur Beseitigung bzw. Bereinigung der betroffenen Komponenten individuell geplant werden.

Prinzipiell ist eine komplette Neuinstallation (Betriebssystem und Anwendersoftware) der infizierten Komponenten zu empfehlen. Dafür kann auch ein vorhandenes, aktuelles Festplatten-Image (System-Backup) verwendet werden.

Vor dem Einspielen eines Images muss geprüft werden, ob der Ablageort des Images nicht auch infiziert ist. Ein Image von einem infizierten Ablageort soll nicht verwendet werden, da es nicht auszuschließen ist, dass auch das Image manipuliert wurde.

Die folgenden Punkte beeinflussen die Vorgehensweise der Bereinigung und sollen in den Überlegungen und Planungen berücksichtigt werden:

- Zustand der Anlagendokumentation (inkl. Netzwerktopologie, Adressen, Konten, usw.)
- Bereinigung im laufenden Betrieb oder in einer Abstellungsphase
- Kontinuierlicher oder Batch Verfahrensprozess
- Redundanzkonzept
- Art der Schadsoftware
- Anzahl der infizierten Rechner
- Infektionsweg

Vorgehenseise

Hinweis

Beachten Sie, dass die beschriebene Vorgehensweise eine beispielhafte Auflistung von möglichen Arbeitsschritten ist, die bei der Bereinigung einer Anlage anfallen können. Diese Auflistung hat keinen Anspruch auf Vollständigkeit. Jeder der aufgelisteten Arbeitsschritte muss detailliert geplant und entsprechend umgesetzt werden.

Die Vorgehensweise nach einer Virusinfektion kann die folgenden Arbeitsschritte enthalten:

- Aufbau/Installation/Implementierung der für die Bereinigung notwendigen zusätzlichen Infrastruktur, z. B.:
  - Ein separates Quarantäne-Netzwerk
  - Ein sichererer Fileserver mit aktuellem Virenscanner (evtl. verschiedene Antivirus-Lösungen) zur Verteilung von Daten
  - Internetzugang mittels separater Workstation mit aktuellem Virenscanner (evtl. verschiedene Antivirus-Lösungen)
- Erfassen aller Netzwerkteilnehmer und ihrer Aufgaben
  Sicherstellen sämtlicher aktueller Daten (Engineering-Daten, Archive, Backups, usw.) pro Teilnehmer.
- Import, Scan, Säuberung und Ablage der aktuellen Daten pro Netzwerkteilnehmer auf dem Fileserver
- Planung der notwendigen Redundanzen (bei einer Bereinigung im laufenden Betrieb)
- Identifikation von Standby-Komponenten, Erstellung eines Speicherabbildes, Analyse und Untersuchung des Speicherabbildes mit dem Ziel der Identifikation der Schadsoftware sowie deren Verbreitungsmechanismus
- Neuinstallation der Komponente entweder von System-Backup (wenn vorhanden und bezüglich einer Infektion unbedenklich) oder mittels Originaldatenträger (Betriebssystem Recovery-CD sowie Automatisierungskomponenten)
- Wiederinbetriebnahme der bereinigten, neuinstallierten Komponenten im "Quarantäne"-Netzwerk als neuen Master
- Transfer der "sauberen" Daten (Engineering-Daten, Archive, Backups, usw.) vom Fileserver auf die bereinigte, neuinstallierte Komponente im "Quarantäne"-Netzwerk
- Überprüfung und Anpassung des Sicherheitskonzepts der Anlage
- Überprüfung und Anpassung des Sicherheitskonzeptes im "Quarantäne"-Netzwerk
- Schrittweiser "Neuaufbau" der Anlage im "Quarantäne"-Netzwerk mit bereinigten, neuinstallierten Komponenten
- Ausbau des "Quarantäne"-Netzwerks zum neuen Automatisierungsnetzwerk mit angepassten Maßnahmen des Sicherheitskonzepts
- Schrittweise Umsetzung der Maßnahmen aus dem Sicherheitskonzept im "Quarantäne"-Netzwerk

Weitere Informationen

Unterstützung bei der Umsetzung bzw. Implementierung eines Virenschutzes in Form von Virenscanner in Ihrer Anlage erhalten Sie bei den Industrial Security Services. Weitere Informationen und die entsprechenden Ansprechpartner finden Sie unter http://www.industry.siemens.com/topics/global/de/industrial-security/seiten/default.aspx.

Sie können Ihre Anfrage auch per E-Mail direkt an "industrialsecurity.i@siemens.com" richten.

Sichern und Wiederherstellen von Daten 8

Um im Fall eines Sicherheitsvorfalls, wie z. B. einer Infektion durch Schadsoftware (siehe Kapitel "Vorgehensweise bei einer Virusinfektion" (Seite 155)) oder eines Ausfalls des Speichermediums (Festplattencrash), das Automatisierungssystem zu bereinigen und somit den reibungslosen und störungsfreien Betrieb so schnell wie möglich wieder herzustellen, ist die regelmäßige Erstellung von Backups notwendig.

Hierbei werden zwei Arten von Backups unterschieden:

- Backup der Engineering-Daten (Projekt-Backup)
- Backup des Systems
  Beim System-Backup wird die Systempartition gesichert. Dies bedeutet, dass das Volume mit den folgenden Daten gesichert wird:
  - Hardwarespezifische Dateien (z. B."Ntldr", "Boot.ini" und "Ntdetect.com")
  - Windows-Betriebssystemdateien
  - Die Installation des Betriebssystems
  - Die Installation aller Programme

8.1 Backup-Strategie

Die Backup-Strategie muss entsprechend den Ausführungen der tiefgestaffelten Verteidigung (Siehe Kapitel "Konzept der tiefgestaffelten Verteidigung – "Defense-in-Depth" (Seite 11)") organisatorisch sowohl für das Projekt-Backup als auch für die System-Backups geplant werden. Dabei sind u.a. die folgenden Punkte zu berücksichtigen:

- Umfang der Backups (für Projekt-Backup und System-Backup)
- Frequenz zur Erstellung von Backups (für Projekt-Backup und System-Backup)
- Ablage bzw. Aufbewahrungsort der Backups
- Archivierung der Backups

8.1.1 Umfang der Backups

Projekt-Backup

Das Projekt-Backup umfasst die gesamten Projektdaten. Dies bedeutet alle Daten, die zu einem SIMATIC PCS 7-Projekt gehören. Diese Daten bzw. das PCS 7 Projekt (Multiprojekt inkl. aller darin enthaltenen Einzelprojekte) lassen sich mit Hilfe des SIMATIC Managers archivieren. Abhängig vom voreingestellten Archivierungsprogramm entsteht bei diesem Vorgang ein ZIP-Archiv, das die gesamten Projektierungsdaten enthält.

Hinweis

Die Schritte zur Erstellung eines Projekt-Backups und die Vorgehensweise im SIMATIC Manager finden Sie im Handbuch "SIMATIC Prozessleitsystem PCS 7 Kompendium Teil A – Projektierungsleitfaden".

System-Backup

Das System-Backup enthält alle Systemdaten für eine spezifische System-Komponente, z. B. für einen OS-Server, einen OS-Client oder eine Engineering Station. Zu diesen Systemdaten gehören u. a:

- Das Betriebssystem, d.h. alle Daten des Betriebssystems (Windows XP, Windows 7, Windows Server 2003 oder 2008R2)
- Alle installierten Programme, z. B. SIMATIC Manager, WinCC
- Alle notwendigen, gerätespezifischen Treiber, z. B. für Grafik, Netzwerk

All diese Daten befinden sich in der Regel auf der Systempartition (C:\). Somit muss das System-Backup ein Backup der gesamten Systempartition (C:\) sein.

8.1.2 Intervall der Backup-Erstellung

Mit dem Backup-Intervall wird festgelegt, wann ein bestimmtes Backup erstellt werden muss. Dabei ist das Intervall von der Art des Backups abhängig. Ein Projekt-Backup muss in der Praxis häufiger (mit einer höheren Frequenz) als ein System-Backup erstellt werden.

Projekt-Backup

Das Projekt-Backup enthält die Projektierungsdaten und ist aus diesem Grund veraltet, wenn eine Projektierungsänderung durchgeführt wird. Den Zyklus zur Erstellung eines Projekt-Backups hängt aus diesem Grund von der Änderungsfrequenz ab und soll dementsprechend festgelegt werden.

System-Backup

Das System-Backup enthält die Systemdaten einer Systemkomponente. Diese Daten werden grundsätzlich im laufenden Betrieb nur sehr selten geändert. Ein mögliches Szenario für eine Änderung wäre die Installation eines zusätzlichen Programms oder eines notwendigen Treibers. Das sind aber administrative Tätigkeiten, die grundsätzlich nicht täglich durchgeführt werden. Aus diesem Grund ist die Häufigkeit zur Erstellung eines System-Backups abhängig von solchen administrativen Eingriffen in einer Systemkomponente.

Eine Besonderheit stellt ein konsequent betriebenes Patchmanagement dar. Wenn z. B. eine neue Software (z. B. ein Sicherheitsupdate oder ein wichtiges Update) auf einer Systemkomponente installiert wird, muss ein aktuelles System-Backup für diese Systemkomponente erstellt werden.

Hinweis

Für SIMATIC PCS 7 ist das Produkt "Symantec System Recovery" auf Verträglichkeit getestet.

8.2 Aufbewahrungsort von Backups

Projekt- sowie auch System-Backups müssen an einem sicheren Ort aufbewahrt werden. Welcher Ort als "sicher" gilt, muss individuell vom Betreiber im Rahmen der organisatorischen Sicherheit (IT Security Management Plan) festgelegt werden. Folgende Punkte sollen bei den Überlegungen berücksichtigt werden:

- Gebäude
- Feuerzonen bzw. Feuerbereiche

8.3 Archivierung

Backups, speziell Projekt-Backups, sollen archiviert werden. Die Festlegungen zur Archivierung von Backups müssen individuell vom Betreiber im Rahmen der organisatorischen Sicherheit (IT Security Management Plan) festgelegt werden.

Hinweis

Informationen zum Thema "Sichern und Wiederherstellen von Daten" finden Sie in folgenden Dokumenten:

- Handbuch "SIMATIC Prozessleitsystem PCS 7 Serviceunterstützung und Diagnose" (http://support.automation.siemens.com/WW/view/de/68157287), Kapitel "Datensicherung"
- Handbuch "SIMATIC Prozessleitsystem PCS 7 Kompendium Teil D – Betriebsführung und Wartung"
- FAQ "Wie kann im laufenden Betrieb eine Sicherung der OS-Systeme erstellt werden?" (http://support.automation.siemens.com/WW/view/de/56897157).

Fernzugriff 9

9.1 Sichere Fernwartung auf Basis der Siemens Remote Service Platform

Einleitung

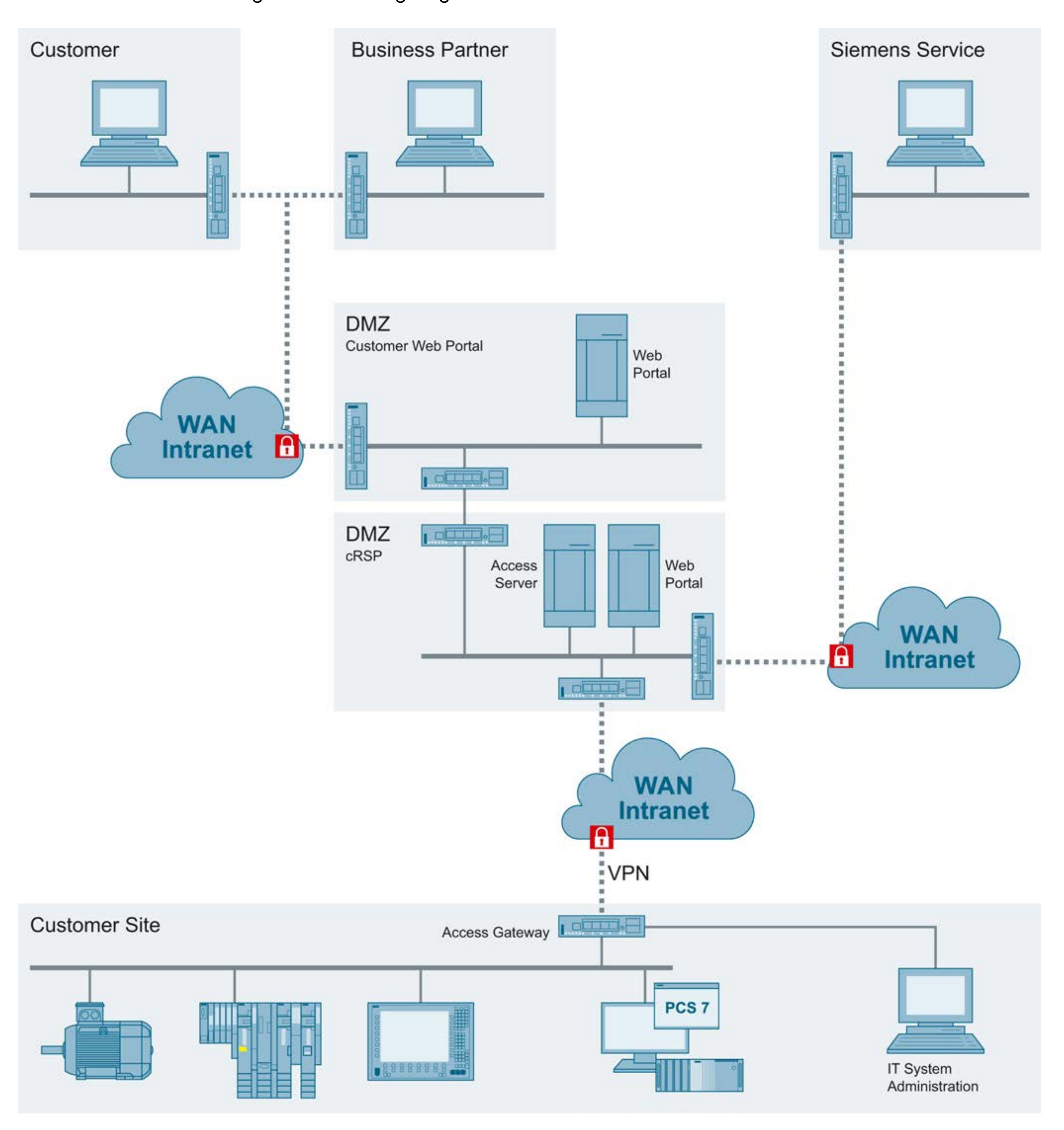
Optimaler proaktiver, systemspezifischer Support für das Automatisierungssystem aus der Ferne: Diese Idee steckt hinter der Siemens Remote Service Platform. Dank ihres modularen Aufbaus können die SIMATIC Remote Services optimal an den tatsächlichen Bedarf angepasst werden. Im Rahmen der angebotenen Module wird nicht nur die Remote Infrastruktur bereitgestellt, auch Support und Wartung sind bereits enthalten.
Da die SIMATIC Remote Services auf der SIEMENS Remote Service (SRS) Platform basieren, arbeiten Anlagenbetreiber mit einer sicheren, performanten und hochverfügbaren Plattform für den Remote-Zugriff auf Ihre SIMATIC-Automatisierungssysteme.

Die Plattform

Die SIMATIC Remote Support Services basieren auf der SIEMENS Remote Service Platform. Damit steht eine sichere, performante und hochverfügbare remote Verbindung zur Verfügung.

- Abgestuftes Sicherheits- und Zugangskonzept
- Collaboration & Customer Web Portal
- Zentrales Monitoring, Logging und Reporting
- E-Mail Benachrichtigung
- Transparente Zugriffe zu jeder Zeit
- Harte Authentifizierung
- Verschlüsselte Kommunikation durch SSL und VPN

Die folgende Abbildung zeigt die Architektur der SIEMENS Remote Service Platform:



9.2 Erstellen eines Remote Service-Konzeptes

Für eine sichere Fernwartung müssen im Vorfeld die wichtigsten Komponenten für den Remote-Zugang identifiziert und verfügbar gemacht werden. Denn durch ein fehlendes Konzept und fehlende Zugriffsmöglichkeiten werden unter Zeit- und Kostendruck meist Sicherheitsrisiken in Kauf genommen und haben damit einen möglichen wirtschaftlichen Schaden zur Folge.

Die folgenden Fragen sollen berücksichtigt werden:

- Welches Equipment benötige ich zur Service Leistungserbringung?
- Wo befindet sich dieses Equipment?
- Wie kann ich dieses Equipment erreichen?
- Welche Werkzeuge (STEP 7, WinCC, SDT, File Transfer…) benötige ich?

Zusätzlich soll auch der Service-Fall betrachtet werden, um im Vorfeld mögliche Probleme bei der Leistungserbringung zu minimieren:

- Wird z.B. das Equipment durch mehrere Personen gleichzeitig benötigt?
- Ist die Service-Tätigkeit rückwirkungsfrei?
- Wer erteilt die Genehmigung für den Remote-Anschluss inkl. Vertreter Regelung?

Wenn diese Fragen beantwortet sind, werden diese Punkte in der SIEMENS Remote Service Platform elektronisch abgebildet und stellen damit einen funktionsfähigen aber auch nach Minimalprinzip eingerichteten Remote Service-Zugang dar. Der Leistungserbringer hat damit die Systeme und Werkzeuge zur Verfügung, die er für die Leistungserbringung benötigt.

Da der Remote Service ein erhöhtes Risiko für Leistungsempfänger wie auch für Leistungserbringer bedeutet, wird diese Zusammenarbeit in einem Service-Vertrag festgehalten und abgesichert.

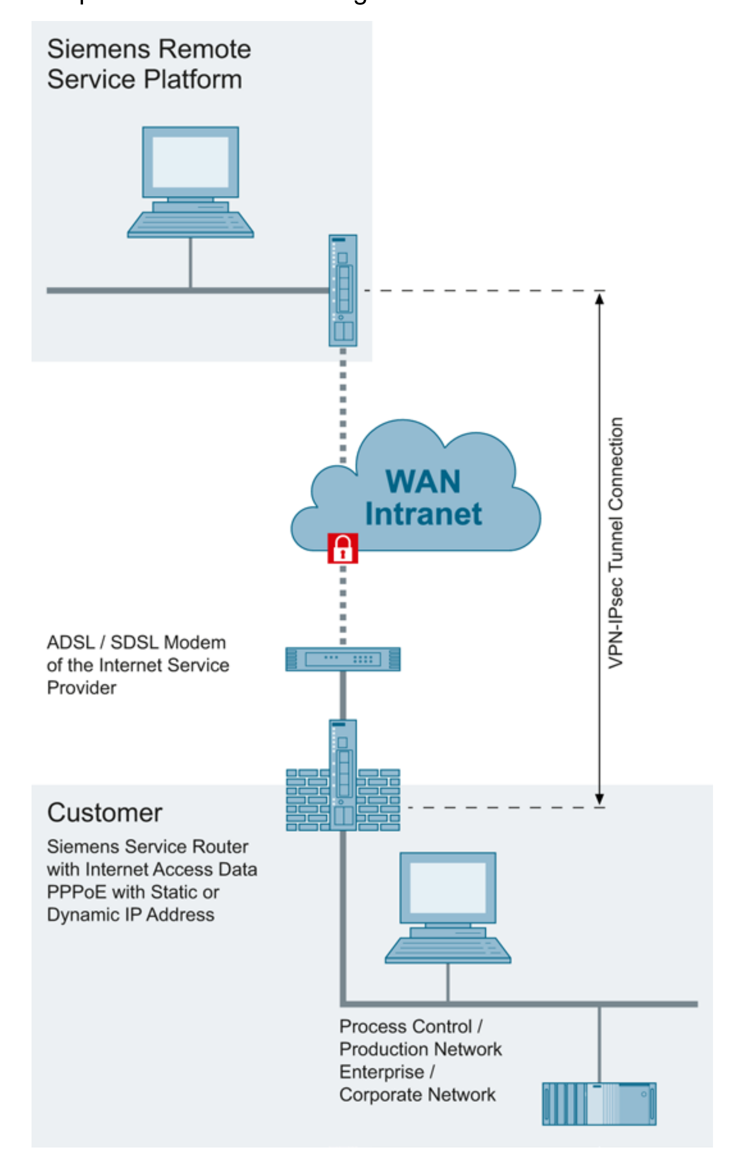
9.3 Anbindungsmöglichkeiten an die Siemens Remote Service Platform

Die SIEMENS Remote Service-Plattform steht als zentrale Infrastruktur zur Verfügung. Die Systeme für eine Fernwartung müssen nur noch angeschlossen werden. Dazu stehen verschiedene Zugangslösungen zu Verfügung.

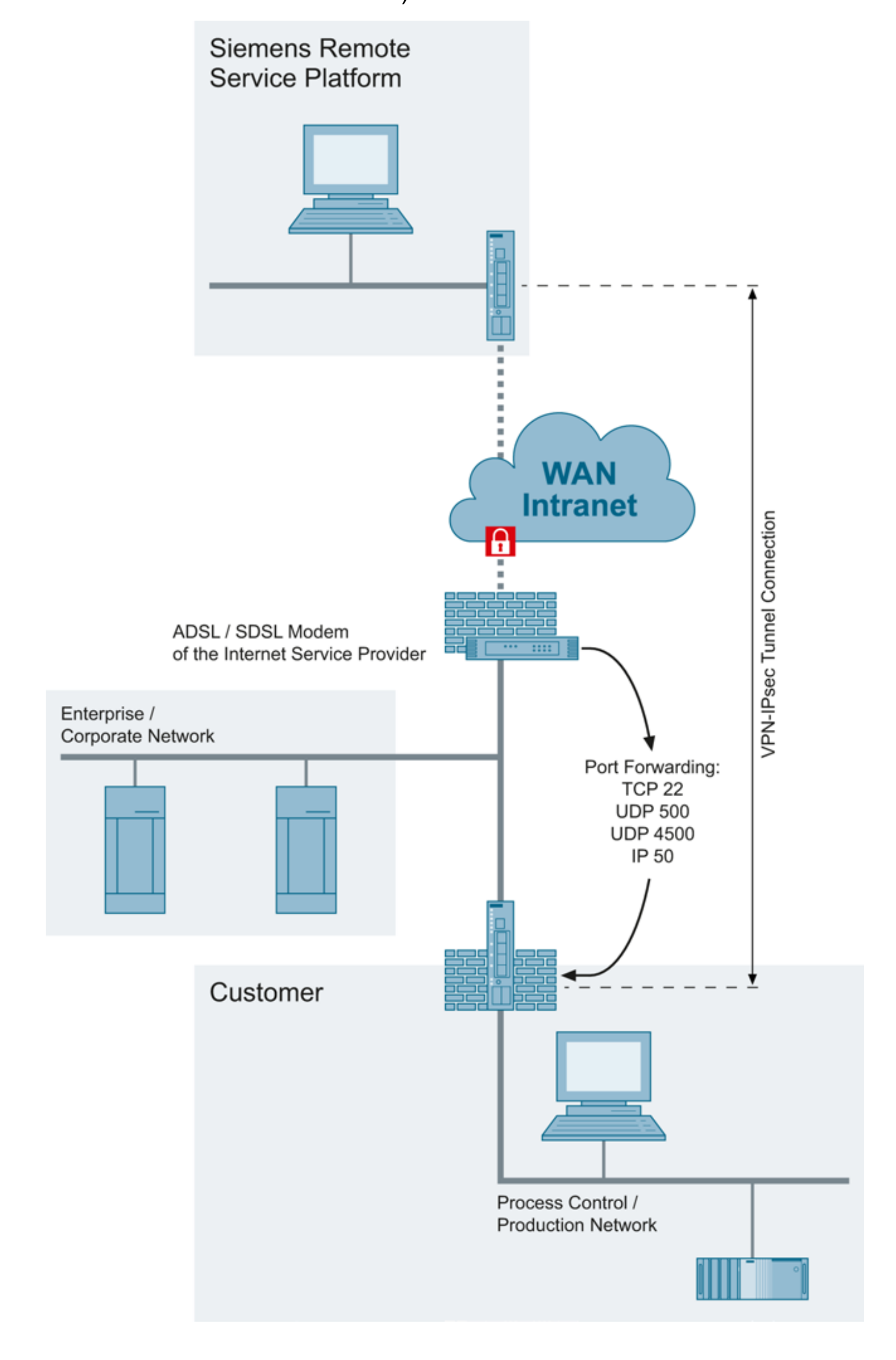
Connectivity Installation (SRS DSL/UMTS access)

Für die Realisierung dieser Lösung gibt es die folgenden Möglichkeiten:

- Internetzugang über ADSL/SDSL Modem
  Es wird ein Service Router geliefert, der mittels ADSL/SDSL-Modem direkt an das Breitbandnetz angebunden wird. Diese Verbindung wird als sicherer Zugang zur Siemens Remote Service Platform verwendet. Die Konfiguration der Zugangsdaten für das PPPoE-Protokoll und Terminierung der VPN-IPsec-Tunnelverbindung erfolgt im Siemens Service Router. Der Siemens Service Router bildet in diesem Fall den IPsec-Tunnel-Endpunkt dieser Verbindung.

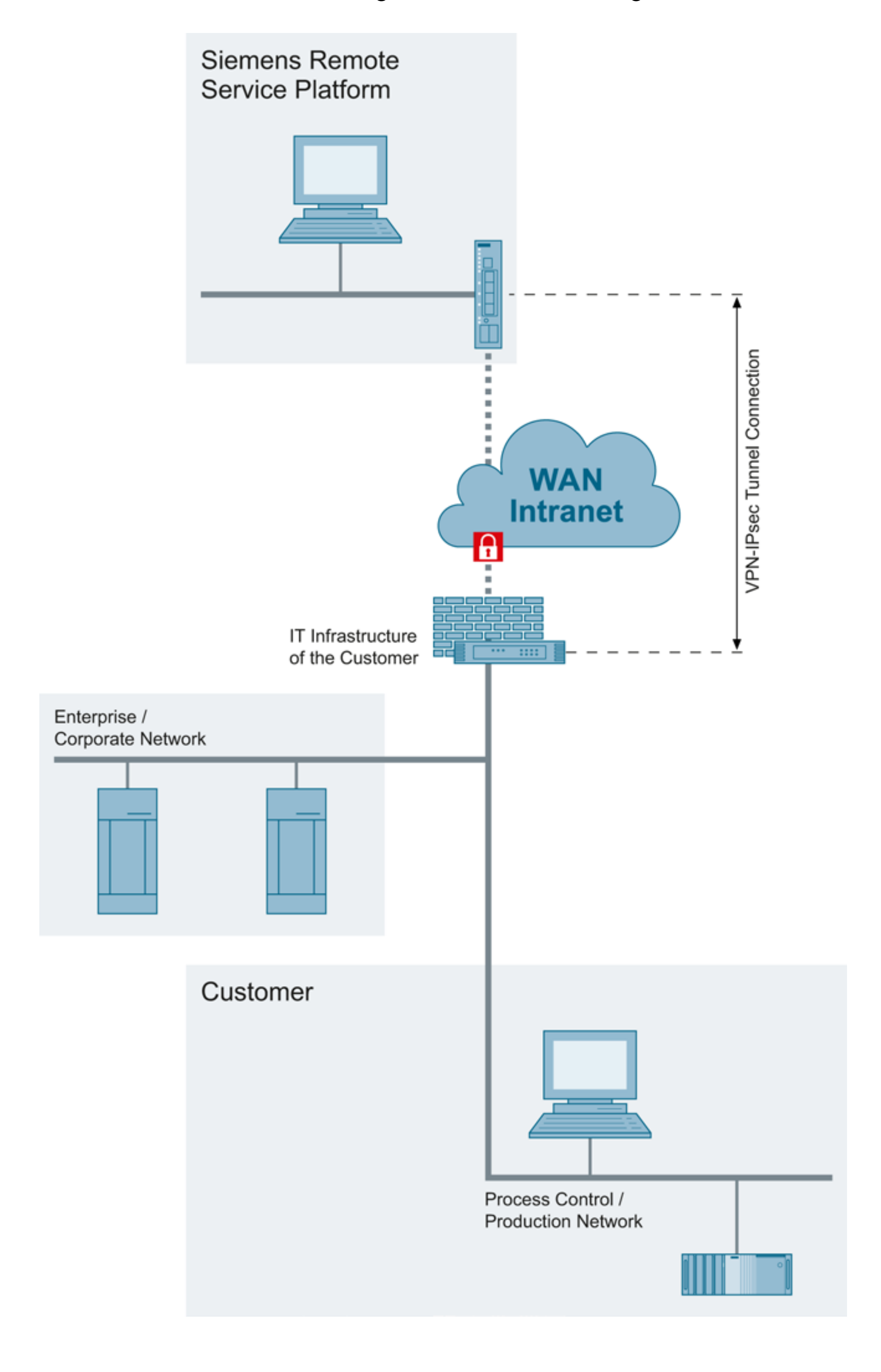


- Nutzung eines bestehenden Internetzugangs
  Es wird ein Service Router geliefert, der mittels eines vorhandenen Internet Access Point an das Breitbandnetz angebunden wird. Diese Verbindung wird als sicherer Zugang zur Siemens Remote Service-Plattform verwendet. Hinter dem Internet Access Point des Kunden wird die VPN-IPsec-Tunnelverbindung terminiert. Der Siemens Service Router bildet in diesem Fall den IPsec-Tunnel-Endpunkt dieser Verbindung. Für die sichere Übermittlung der Daten ist eine Weiterleitung der IPSec geschützten Daten vom Internet Access Point des Kunden zum Siemens Service Router erforderlich (Portweiterleitung zum SIEMENS Service Router).



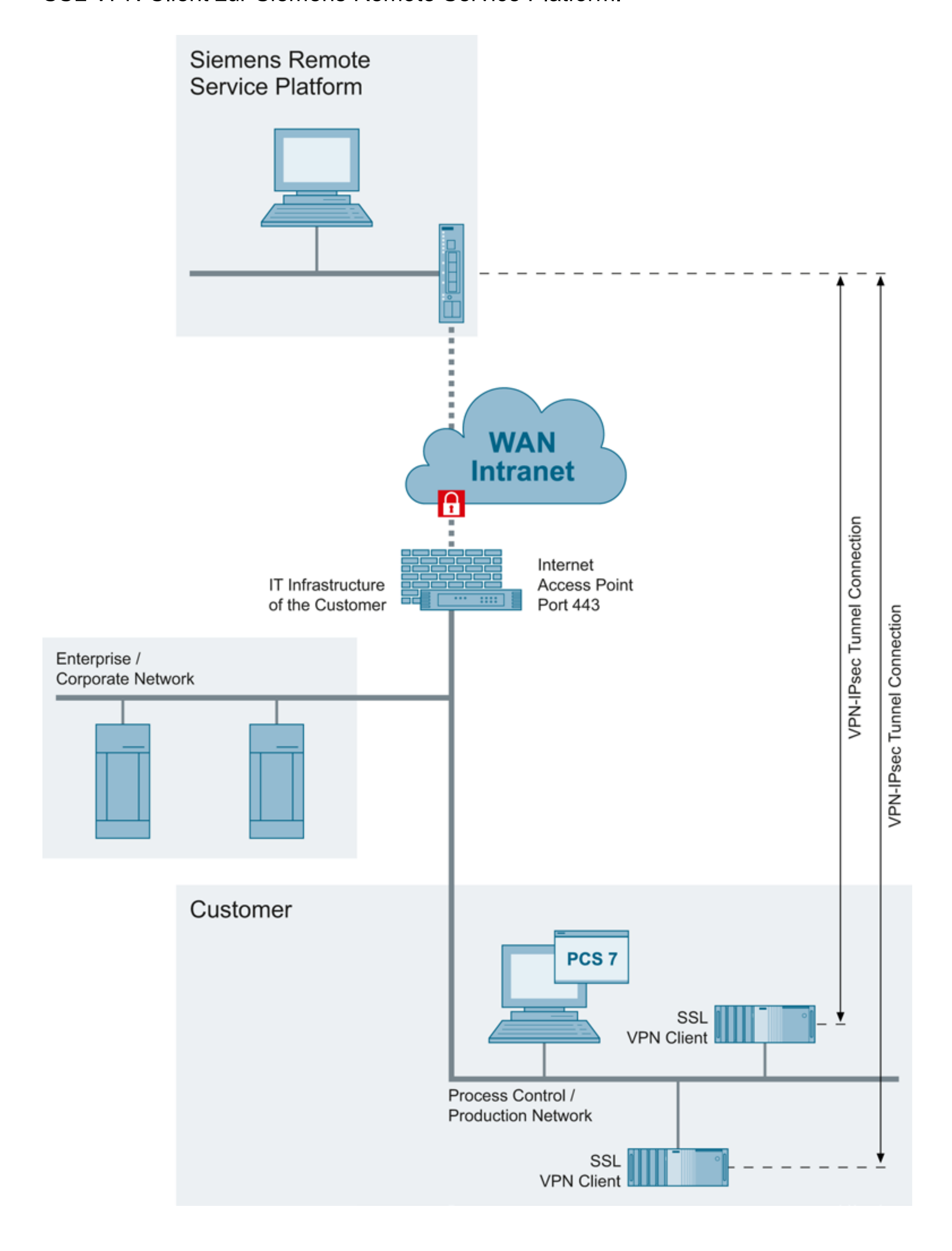
Connectivity Installation (SRS Customer own access)

Eine existierende IT-Infrastruktur wird als Verbindungspartner zur Siemens Remote Service-Plattform verwendet. Im IT-Equipment des Kunden erfolgt die Terminierung für die notwendige VPN IPsec-Tunnelverbindung. Für die sichere Übermittlung der Daten ist ein konformer Standard-IPsec-Endpunkt zur Verfügung zu stellen, bei dem eine Preshard Secret basierender IPsec-Verbindung im Tunnelmodus eingerichtet werden kann.



Connectivity Installation (SRS SSL client access)

Es wird eine SSL VPN Client-Software bereitgestellt, die mittels vorhandener IT-Infrastruktur über einen Internetzugang (Port 443) eine Verbindung zur Siemens Remote Service Platform herstellt. Hinter dem Internetzugang wird die VPN-IPsec-Tunnelverbindung am Client System terminiert. Der auf dem Zielsystem installierte SSL VPN Client bildet in diesem Fall den IPsec-Tunnel-Endpunkt dieser Verbindung. Der Verbindungsaufbau erfolgt vom SSL VPN Client zur Siemens Remote Service Platform.



Definitionen und Abkürzungen 10

Die folgende Tabelle zeigt die im Dokument verwendeten Abkürzungen:

Abkürzung	Erläuterung
Active Directory	Verzeichnisdienst von Microsoft Windows Server
CSN	Control System Network (Anlagenbus)
DC	Domain Controller
DCS	Distributed Control System
DMZ	Demilitarisierte Zone
DNS	Domain Name System
ECN	Enterprise Control Network
ERP	Enterprise Resource Planning
ES	PCS 7 Engineering Station
IANA	Internet Assigned Numbers Authority
MES	Manufacturing Execution System
MON	Manufacturing Operations Network
MS	Microsoft
OS-Client	PCS 7 Operator Station; Ausführung Client
OS-Server	PCS 7 Operator Station; Ausführung Server
PCN	Process Control Network (Terminalbus)
PCN1	Produktionszelle 1
PCN2	Produktionszelle 2
PCS 7	Process Control System der Firma Siemens
PN	Perimeter Netzwerk
SC	Security Controller
SCT	Security Configuration Tool
SSC	SIMATIC Security Control
TMG	Microsoft Forefront Threat Management Gateway
WINS	Windows Internet Naming Service
WSUS	Windows Server Update Services